

QIDs Fixed to Remove Incorrect Exploit References

QID	Vulnerability Title	Severity	Vulnerability Type
100036	Microsoft Cumulative Security Update for Internet Explorer (MS06-042)	Vulnerability - level 5	Vuln
100037	Cumulative Security Update for Internet Explorer (MS06-042 and KB923762)	Vulnerability - level 5	Vuln
100058	Microsoft Internet Explorer Cumulative Security Update (MS08-031)	Vulnerability - level 4	Vuln
100083	Microsoft Internet Explorer Cumulative Security Update (MS10-018 and KB981374)	Vulnerability - level 5	Vuln
100098	Microsoft Internet Explorer 8 Multiple Unspecified Vulnerabilities (Deprecated)	Vulnerability - level 4	Vuln
100099	Microsoft Internet Explorer Cumulative Security Update (MS11-018)	Vulnerability - level 4	Vuln
100116	Microsoft Internet Explorer Cumulative Security Update (MS12-037)	Vulnerability - level 4	Vuln
100127	Microsoft Internet Explorer Cumulative Security Update (MS12-063) (SA2757760)	Vulnerability - level 5	Vuln
100142	Microsoft Internet Explorer Multiple Remote Code Execution Vulnerabilities (MS13-021)	Vulnerability - level 5	Vuln
100152	Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10 (KB2833510)	Vulnerability - level 4	Vuln
100188	Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer (KB2942844)	Vulnerability - level 4	Vuln
100192	Microsoft Internet Explorer Cumulative Security Update (MS14-037)	Vulnerability - level 5	Vuln
100276	Microsoft Cumulative Security Update for Internet Explorer (MS16-009)	Vulnerability - level 4	Vuln
100291	Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer (MS16-093)	Vulnerability - level 5	Vuln
105728	EOL/Obsolete Software: Apache HTTP Server 2.2.x Detected	Vulnerability - level 5	Practice
110034	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS06-037)	Vulnerability - level 4	Vuln
110038	Microsoft PowerPoint Remote Code Execution Vulnerabilities (MS06-048)	Vulnerability - level 4	Vuln
110090	Microsoft Excel Multiple Remote Code Execution Vulnerabilities (MS08-074)	Vulnerability - level 4	Vuln
110092	Microsoft Word Multiple Remote Code Execution Vulnerabilities (MS08-072)	Vulnerability - level 4	Vuln
110100	Microsoft Excel Remote Code Execution Vulnerability (MS09-021)	Vulnerability - level 4	Vuln
110109	Microsoft PowerPoint Remote Code Execution Vulnerability (MS10-004)	Vulnerability - level 4	Vuln
110113	Microsoft Office Remote Code Execution Vulnerability (MS10-003)	Vulnerability - level 4	Vuln
110160	Microsoft Office Remote Code Execution Vulnerability (MS12-030)	Vulnerability - level 4	Vuln
110192	Microsoft Word Remote Code Execution Vulnerability (MS12-064)	Vulnerability - level 5	Vuln
110195	Microsoft Excel Remote Code Execution Vulnerabilities (MS12-076)	Vulnerability - level 4	Vuln
110297	Microsoft Office and Microsoft Office Services and Web Apps Security Update April 2017	Vulnerability - level 4	Vuln
115071	Red Hat Update for tomcat (RHSA-2015:0983)	Vulnerability - level 3	Vuln
115075	Red Hat Update for tomcat6 (RHSA-2015:0991)	Vulnerability - level 3	Vuln
115082	Red Hat Update for java-1.7.0-ibm (RHSA-2015:1007)	Vulnerability - level 5	Vuln
115083	Red Hat Update for java-1.6.0-ibm (RHSA-2015:1006)	Vulnerability - level 5	Vuln
115089	Solaris 11.2 Support Repository Update (SRU) 10.5.0 Missing	Vulnerability - level 3	Vuln
115093	Fedora Security Update for mingw-openssl (FEDORA-2015-6855)	Vulnerability - level 3	Vuln

11512	Splunk Enterprise and Splunk Light Multiple Vulnerabilities (SP-CAAN84)	Potential Vulnerability - level 3	Practice
11512	Window Maker Unspecified WMGLOBAL Vulnerability	Potential Vulnerability - level 3	
115138	Fedora Security Update for wpa_supplicant (FEDORA-2015-6952)	Vulnerability - level 3	Vuln
115163	Red Hat Update for java-1.5.0-ibm (RHSA-2015:1021)	Vulnerability - level 4	Vuln
115164	Red Hat Update for java-1.7.1-ibm (RHSA-2015:1020)	Vulnerability - level 5	Vuln
115166	Google Chrome Diffie-Hellman Weak Encryption Vulnerability (Logjam)	Vulnerability - level 4	Vuln
115167	Mozilla Firefox Diffie-Hellman Weak Encryption Vulnerability (Logjam) ((MFSa 2015-59 to MFSa 2015-71)	Vulnerability - level 4	Vuln
115168	Apple Safari Diffie-Hellman Weak Encryption Vulnerability (Logjam)	Vulnerability - level 4	Vuln
115169	Opera Diffie-Hellman Weak Encryption Vulnerability (Logjam)	Vulnerability - level 4	Vuln
115190	Docker Secure Sockets Layer/Transport Layer Security (SSL/TLS) Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
115226	Red Hat Update for openssl (RHSA-2015:1072)	Vulnerability - level 3	Vuln
115241	CentOS Security Update for tomcat6 (CESA-2015:0991)	Vulnerability - level 3	Vuln
115245	CentOS Security Update for tomcat (CESA-2015:0983)	Vulnerability - level 3	Vuln
115254	CentOS Security Update for openssl (CESA-2015:1072)	Vulnerability - level 3	Vuln
115257	OpenSSL Diffie-Hellman Weak Encryption Vulnerability (Logjam)	Vulnerability - level 4	Practice
115299	Apple QuickTime Multiple Vulnerabilities (APPLE-SA-2005-11-04)	Vulnerability - level 4	Vuln
115305	Apple Mac OS X Security Update 2005-009 Not Installed (APPLE-SA-2005-11-29)	Vulnerability - level 3	Vuln
115311	Apple Mac OS X Perl Insecure Privilege Dropping Weakness	Vulnerability - level 3	Vuln
115317	OpenSSH Local SCP Shell Command Execution Vulnerability (FEDORA-2006-056, Vmware-3069097-Patch, Vmware-9986131-Patch)	Vulnerability - level 3	Practice
115318	Linux Kernel Multiple Security Vulnerabilities	Potential Vulnerability - level 3	Practice
115329	GNUTLS LibTASN1 DER Decoding Denial of Service Vulnerabilities	Vulnerability - level 3	Vuln
115334	Apple Mac OS X Security Update 2006-001 Not Installed (APPLE-SA-2006-03-01)	Vulnerability - level 3	Vuln
115335	GNU Tar Invalid Headers Buffer Overflow Vulnerability	Potential Vulnerability - level 3	Practice
115354	Mozilla SeaMonkey Multiple Vulnerabilities	Vulnerability - level 4	Vuln
115355	HP-UX running TCP/IP Remote Denial of Service Vulnerability (HPSBUX02087)	Vulnerability - level 3	Vuln
115357	Apple Mac OS X Security Update 2006-003 Not Installed (APPLE-SA-2006-05-11)	Vulnerability - level 3	Vuln
115422	Apple Mac OS X 10.4.8 and Security Update 2006-006 Not Installed (APPLE-SA-2006-09-29)	Vulnerability - level 4	Vuln
115456	Red Hat texinfo Security Update (RHSA-2006:0727)	Vulnerability - level 3	Vuln
115471	Apple Mac OS X Security Update 2006-007 Not Installed (APPLE-SA-2006-11-28)	Vulnerability - level 5	Vuln
115527	Apple Mac OS X 10.4.9 and Security Update 2007-003 Not Installed (APPLE-SA-2007-03-13)	Vulnerability - level 5	Vuln
115533	VMware ESX Server 3.0/3.0.1 Multiple Vulnerabilities	Vulnerability - level 5	Vuln
115539	Apple Mac OS X Security Update 2007-004 Not Installed (APPLE-SA-2007-04-19)	Vulnerability - level 4	Vuln
115656	Apple QuickTime 7.3 Not Installed	Vulnerability - level 4	Vuln
115674	Skype Technologies skype4com URI Handler Remote Heap Corruption Vulnerability	Vulnerability - level 4	Vuln
115676	Apple Mac OS X Security Update 2007-009 Not Installed (APPLE-SA-2007-12-17)	Vulnerability - level 5	Vuln
115679	Adobe Flash Player Multiple Vulnerabilities (APSB07-20)	Vulnerability - level 4	Vuln
115748	Macrovision InstallShield Update Service Multiple Insecure Methods	Vulnerability - level 4	Vuln
115754	Apple Security Update 2008-002 Not Installed	Vulnerability - level 4	Vuln

115757	Red Hat krb5 Security Update (RHSA-2008:0180,RHSA-2008:0181)	Vulnerability - level 3	Vuln
115759	Red Hat unzip Security Update (RHSA-2008:0196)	Vulnerability - level 3	Vuln
115767	SUSE Security Announcement: krb5 (SUSE-SA:2008:016)	Vulnerability - level 3	Vuln
115785	Apple Safari Multiple Vulnerabilities (SA-2008-04-16)	Vulnerability - level 4	Vuln
115800	Sun Solaris Security Issues in Tcl GUI Toolkit Library May Lead to Denial of Service (1019237.1)	Vulnerability - level 3	Vuln
115801	Adobe Acrobat and Adobe Reader Multiple Vulnerabilities (APSB08-13)	Vulnerability - level 4	Vuln
115802	Debian OpenSSL Predictable Random Number Generator Update	Vulnerability - level 4	Vuln
115804	Red Hat Kernel Security Update	Vulnerability - level 3	Vuln
115812	Apple Mac OS X 10.5.3 and Security Update 2008-003 Not Installed (APPLE-SA-2008-05-28)	Vulnerability - level 4	Vuln
115824	VMware Security Update (VMSA-2008-0008 and VMSA-2008-0009)	Vulnerability - level 5	Vuln
115829	Apple Quicktime Multiple Vulnerabilities (APPLE-SA-2008-06-09)	Vulnerability - level 4	Vuln
115848	Apple Mac OS X 10.5.4 and Security Update 2008-004 Not Installed (APPLE-SA-2008-06-30)	Vulnerability - level 4	Vuln
11585	Elasticsearch transport.tcp.port Remote Code Execution Vulnerability	Potential Vulnerability - level 4	Practice
11585	Minihttp Forum Web Server Plain Text Password Storage Vulnerability	Potential Vulnerability - level 4	
115851	Mozilla Firefox and SeaMonkey Multiple Vulnerabilities	Vulnerability - level 4	Vuln
115852	VLC Media Player WAV Processing Integer Overflow	Vulnerability - level 4	Vuln
115854	Red Hat Pidgin Security and Bug Fix Update (RHSA-2008:0584-2)	Vulnerability - level 3	Vuln
11587	Elasticsearch CORS Information Disclosure Vulnerability	Potential Vulnerability - level 3	Practice
11587	Goollery Multiple Cross-Site Scripting Vulnerabilities	Potential Vulnerability - level 3	
115884	Red Hat Kernel Security Update (RHSA-2008:0612)	Vulnerability - level 3	Vuln
115889	Solaris Security Issue in FreeType2 Library May Lead to Denial of Service (1019380.1)	Vulnerability - level 3	Vuln
115891	Security Vulnerability in Perl Version 5.8	Vulnerability - level 3	Vuln
115928	VMware Security Update (VMSA-2008-0014)	Vulnerability - level 4	Vuln
115936	Solaris GNU tar Denial of Service Vulnerability (1019583.1)	Vulnerability - level 3	Vuln
115956	LANDesk Multiple Products Buffer Overflow Vulnerability	Vulnerability - level 3	Vuln
115976	Red Hat Update for pam_krb5 (RHSA-2008:0907)	Vulnerability - level 2	Vuln
115983	Apple Mac OS X Security Update 2008-007 Not Installed (APPLE-SA-2008-10-09)	Vulnerability - level 4	Vuln
116014	Fedora Update for Drupal	Vulnerability - level 3	Vuln
116016	Red Hat Update for Flash-Plugin(RHSA-2008:0945)	Vulnerability - level 3	Vuln
116027	Adobe Acrobat/Reader "util.printf()" Buffer Overflow Vulnerability (APSB08-19)	Vulnerability - level 4	Vuln
116038	Adobe Flash Player Multiple Security Issues and Vulnerabilities (APSB08-18)	Vulnerability - level 3	Vuln
116121	Red Hat Update for xterm (RHSA-2009:0018)	Vulnerability - level 3	Vuln
116128	Red Hat Update for squirrelmail (RHSA-2009:0010-6)	Vulnerability - level 3	Vuln
116142	Fedora Update for drupal (FEDORA-2009-0678)	Vulnerability - level 4	Vuln
116147	Trend Micro OfficeScan Client Firewall Multiple Vulnerabilities	Vulnerability - level 3	Vuln
11615	Software602 602 LAN Suite Multiple Remote Denial Of Service Vulnerabilities	Vulnerability - level 3	
11615	Splunk Enterprise and Light Multiple Vulnerabilities. (SP-CAAAPKV)	Vulnerability - level 3	Vuln
116160	CA (Computer Associates) Antivirus Engine "arclib.dll" Multiple Scan Evasion Vulnerabilities	Vulnerability - level 3	Vuln
116164	AXIS Camera Control image_pan_tilt Property Buffer Overflow	Vulnerability - level 4	Vuln
116174	Sun Java Multiple Vulnerabilities	Vulnerability - level 4	Vuln
116180	SAP GUI TabOne ActiveX Control Caption List Buffer Overflow	Vulnerability - level 4	Vuln
11619	Meteocontrol WEB'log Basic 100, Light, Pro, and Pro Unlimited Multiple Vulnerabilities	Vulnerability - level 5	Vuln

11619	Sun Java Runtime Environment InitialDirContext Remote Denial Of Service Vulnerability	Vulnerability - level 5	
116191	HP-UX Running IPv6, Remote Denial of Service Vulnerability (HPSBUX02407)	Vulnerability - level 3	Vuln
116213	Java for Mac OS X 10.4 Release 8 (APPLE-SA-2009-02-12)	Vulnerability - level 3	Vuln
116215	Apple Mac OS X Security Update 2009-001 Not Installed (APPLE-SA-2009-02-12)	Vulnerability - level 4	Vuln
116255	Winamp libsndfile.dll CAF Processing Integer Overflow Vulnerability	Vulnerability - level 4	Vuln
116273	Foxit Reader 3.0 Build 1506 Security Update	Vulnerability - level 4	Vuln
116314	Red Hat Update for IBMJava2 (RHSA-2007:0072-2)	Vulnerability - level 3	Vuln
116315	Critical Security Updates for all Supported Versions of VMware ESX Server VMware Server VMware Workstation VMware ACE and VMware Player (VMSA-2007-0006)	Vulnerability - level 3	Vuln
116332	Red Hat Update for openswan (RHSA-2009:0402-1)	Vulnerability - level 3	Vuln
116343	UltraISO Multiple Disk Image Parsing Vulnerabilities	Vulnerability - level 3	Vuln
116351	IrfanView Formats Plug-in XPM Parsing Integer Overflow Vulnerability	Vulnerability - level 4	Vuln
116355	Fedora Update for mapserver (FEDORA-2009-3383,FEDORA-2009-3357)	Vulnerability - level 3	Vuln
116370	PGP Desktop "pgpdisk.sys" Local Denial of Service Vulnerability	Vulnerability - level 3	Vuln
116375	Red Hat Update for krb5 (RHSA-2009:0408)	Vulnerability - level 3	Vuln
116383	VMware Multiple Denial of Service Vulnerabilities(VMSA-2007-0004)	Vulnerability - level 3	Vuln
116419	Garmin Communicator Plug-In Domain Locking Security Bypass Vulnerability	Vulnerability - level 3	Vuln
116423	Apple Mac OS X 10.5.7 and Security Update 2009-002 Not Installed (APPLE-SA-2009-05-12)	Vulnerability - level 4	Vuln
116436	Sun Solaris "sadmind" Multiple Vulnerabilities (1020498.1)	Vulnerability - level 5	Vuln
116440	Java for Mac OS X 10.5 Update 4 and Java for Mac OS X 10.4 Release 9 (APPLE-SA-2009-06-15-1, APPLE-SA-2009-06-15-2)	Vulnerability - level 4	Vuln
116443	Apple QuickTime 7.6.2 Not Installed	Vulnerability - level 4	Vuln
116453	Apple Safari 4.0 Not Installed	Vulnerability - level 4	Vuln
116455	Adobe Reader and Acrobat Security Update (APSB09-07)	Vulnerability - level 4	Vuln
116487	VMWare ESX Service Console Update for krb5 (VMSA-2009-0008)	Vulnerability - level 4	Vuln
116489	SUSE Update for acroread (SUSE-SA:2009:035)	Vulnerability - level 3	Vuln
116521	Fedora Update for libtiff (FEDORA-2009-7724, FEDORA-2009-7775)	Vulnerability - level 4	Vuln
116541	Fedora Update for xml-security-c (FEDORA-2009-8121, FEDORA-2009-8157)	Vulnerability - level 3	Vuln
116547	Apple Mac OS X 10.5.8 and Security Update 2009-003 Not Installed (APPLE-SA-2009-08-05-1)	Vulnerability - level 4	Vuln
116569	Red Hat Subversion Security Update (RHSA-2009:1203-1)	Vulnerability - level 3	Vuln
116575	VMware Hosted Products Update libpng and Apache HTTP Server (VMSA-2009-0010)	Vulnerability - level 3	Vuln
116586	CA (Computer Associates) Internet Security Suite Denial of Service	Vulnerability - level 2	Vuln
116588	CA (Computer Associates) Host-Based Intrusion Prevention System Remote Denial of Service	Vulnerability - level 2	Vuln
11660	Drupal Core Highly Critical Guzzle Vulnerability (SA-CORE-2016-003)	Vulnerability - level 3	Vuln
11660	Phorum FOLLOW.PHP SQL Injection Vulnerability	Vulnerability - level 3	
116601	OpenOffice.org Word Document Table Parsing Buffer Overflow Vulnerability	Vulnerability - level 3	Vuln
116603	Java for Mac OS X 10.5 Update 5 (APPLE-SA-2009-09-03-1)	Vulnerability - level 4	Vuln
116604	Asterisk IAX2 Call Number Exhaustion Denial of Service Vulnerability (AST-2009-006)	Vulnerability - level 2	Vuln
11662	CGI Web Servers Assign Proxy Header Values From Client Vulnerability (HTTProxy)	Vulnerability - level 4	Vuln
11662	ZoneLabs IMsecure URI Filter Bypass Vulnerability	Vulnerability - level 4	

116633	Red Hat Application Stack v2.2 Security and Enhancement Update (RHSA-2008:0966-15)	Vulnerability - level 3	Vuln
116647	VMware ESX Patches for DHCP, Service Console Kernel, and JRE (VMSA-2009-0014)	Vulnerability - level 3	Vuln
116687	Fedora Update for squidGuard (FEDORA-2009-10743, FEDORA-2009-10780)	Vulnerability - level 2	Vuln
116692	Apple Mac OS X 10.6.2 and Security Update 2009-006 Not Installed (APPLE-SA-2009-11-09-1)	Vulnerability - level 4	Vuln
116719	VMware ESX 3.x Update for multiple packages (VMSA-2009-0016)	Vulnerability - level 3	Vuln
116732	Red Hat Update for BIND (RHSA-2009:1620-1)	Vulnerability - level 2	Vuln
116743	Fedora Update for BIND (FEDORA-2009-12218, FEDORA-2009-12233)	Vulnerability - level 2	Vuln
116744	Fedora Update for tomcat6 (FEDORA-2009-11356, FEDORA-2009-11374, FEDORA-2009-11352)	Vulnerability - level 3	Vuln
116748	Adobe Flash Player and AIR Multiple Remote Vulnerabilities (APSB09-19)	Vulnerability - level 3	Vuln
116751	Microsoft Windows Indeo Codec Could Allow Remote Code Execution (KB954157)	Vulnerability - level 4	Vuln
116763	Fedora Update for PHP (FEDORA-2009-12017)	Vulnerability - level 3	Vuln
116768	Adobe Reader and Acrobat Vulnerability (APSA09-07, APSB10-02)	Vulnerability - level 5	Vuln
116785	Red Hat Update for gd (RHSA-2010:0003)	Vulnerability - level 3	Vuln
116794	Java Runtime Environment ImagingLib Buffer Overflow Vulnerability (Oracle Java Critical Patch Update - March 2010)	Vulnerability - level 4	Vuln
116795	Linux Kernel "ebtables" Security Bypass Vulnerability	Vulnerability - level 3	Vuln
116799	Red Hat Update for PHP (RHSA-2010:0040)	Vulnerability - level 3	Vuln
116818	Apple Mac OS X Security Update 2010-001 Not Installed (APPLE-SA-2010-01-19-1)	Vulnerability - level 4	Vuln
116819	Adobe Shockwave Player Buffer Overflow and Integer Overflow Vulnerabilities (APSB10-03)	Vulnerability - level 3	Vuln
116821	RealPlayer Multiple Vulnerabilities	Vulnerability - level 3	Vuln
116822	Red Hat Linux Kernel "qla2xxx" Driver Security Bypass Vulnerability (RHSA-2010:0046)	Vulnerability - level 2	Vuln
116832	CentOS Security Update for gd (CESA-2010:0003)	Vulnerability - level 3	Vuln
116838	Red Hat Update for libtiff (RHSA-2009:1159-1)	Vulnerability - level 3	Vuln
116847	Fedora Update for Kernel (FEDORA-2010-0919)	Vulnerability - level 4	Vuln
116850	Fedora Update for Samba (FEDORA-2010-1190, FEDORA-2010-1218)	Vulnerability - level 2	Vuln
116852	Feodra Update for ncpfs (FEDORA-2010-1145, FEDORA-2010-1168)	Vulnerability - level 2	Vuln
116855	CentOS Security Update for PHP (CESA-2010:0040)	Vulnerability - level 3	Vuln
116864	Asterisk "FaxMaxDatagram" Remote Denial of Service Vulnerability (AST-2010-001)	Vulnerability - level 2	Vuln
116873	Fedora Update for PHP (EDORA-2010-0495)	Vulnerability - level 3	Vuln
116889	Red Hat Update for HelixPlayer (RHSA-2010:0094-1)	Vulnerability - level 4	Vuln
116892	OpenOffice.org Multiple Vulnerabilities	Vulnerability - level 3	Vuln
116895	Fedora update for Bugzilla (FEDORA-2010-1458)	Vulnerability - level 2	Vuln
116898	Fedora Update for Kernel (FEDORA-2010-1804)	Vulnerability - level 3	Vuln
116903	Mozilla Firefox, Thunderbird, SeaMonkey Multiple Vulnerabilities (MFSA 2010-01,MFSA 2010-02,MFSA 2010-03,MFSA 2010-04,MFSA 2010-05)	Vulnerability - level 4	Vuln
116905	CentOS Security Update for Kernel (CESA-2010:0046)	Vulnerability - level 3	Vuln
116908	CentOS Security Update for HelixPlayer (CESA-2010:0094)	Vulnerability - level 3	Vuln
116909	CentOS Security Update for OpenOffice.org (CESA-2010:0101)	Vulnerability - level 3	Vuln
116910	CentOS Security Update for MySQL (CESA-2010:0110)	Vulnerability - level 3	Vuln
116911	CentOS Security Update for SeaMonkey (CESA-2010:0113)	Vulnerability - level 3	Vuln
116912	CentOS Security Update for Firefox (CESA-2010:0112)	Vulnerability - level 4	Vuln
116931	CentOS Security Update for bind (CESA-2009:1620)	Vulnerability - level 3	Vuln
116971	VMware ESX Service Console and vMA Third Party Updates (VMSA-2010-0004)	Vulnerability - level 4	Vuln
117002	CentOS Security Update for xmlsec1 (CESA-2009:1428)	Vulnerability - level 3	Vuln

117004	CentOS Security Update for openoffice.org (CESA-2009:1426)	Vulnerability - level 3	Vuln
117029	CentOS Security Update for Kernel (CESA-2009:1193)	Vulnerability - level 4	Vuln
117036	CentOS Security Update for Java (CESA-2009:1201)	Vulnerability - level 4	Vuln
117039	CentOS Security Update for Subversion (CESA-2009:1203)	Vulnerability - level 4	Vuln
117061	CentOS Security Update for Tomcat (CESA-2009:1164)	Vulnerability - level 4	Vuln
117079	Solaris BIND DNSSEC Software Bogus NXDOMAIN Responses Vulnerability (1021798.1)	Vulnerability - level 2	Vuln
117080	Red Hat Update for Kernel (RHSA-2010:0146,RHSA-2010:0147)	Vulnerability - level 3	Vuln
117105	CentOS Security Update for gpdf (CESA-2009:0458)	Vulnerability - level 4	Vuln
117109	CentOS Security Update for Poppler (CESA-2009:0480)	Vulnerability - level 4	Vuln
117117	CentOS Security Update for Kernel (CESA-2010:0146)	Vulnerability - level 4	Vuln
117118	CentOS Security Update for Thunderbird (CESA-2010:0154)	Vulnerability - level 3	Vuln
117119	CentOS Security Update for kernel (CESA-2010:0147)	Vulnerability - level 4	Vuln
11712	Opera Web Browser Java Implementation Multiple Remote Vulnerabilities	Potential Vulnerability - level 3	
11712	Red Hat JBoss Enterprise Application Platform Multiple Security Vulnerabilities (RHSA-2014:0170-1)	Potential Vulnerability - level 3	Practice
117121	CentOS Security Update for kdegraphics (CESA-2009:0431)	Vulnerability - level 4	Vuln
117129	CentOS Security Update for FreeType (CESA-2009:0329)	Vulnerability - level 4	Vuln
117141	CentOS Security Update for CUPS (CESA-2009:0429)	Vulnerability - level 4	Vuln
117142	CentOS Security Update for Xpdf (CESA-2009:0430)	Vulnerability - level 4	Vuln
117148	CentOS Security Update for krb5 (CESA-2009:0410)	Vulnerability - level 5	Vuln
117149	CentOS Security Update for krb5 (CESA-2009:0409)	Vulnerability - level 4	Vuln
117151	CentOS Security Update for krb5 (CESA-2009:0408)	Vulnerability - level 4	Vuln
117155	CentOS Security Update for Openswan (CESA-2009:0402)	Vulnerability - level 4	Vuln
117178	CentOS Security Update for Hanterm (CESA-2009:0019)	Vulnerability - level 4	Vuln
117182	CentOS Security Update for kernel (CESA-2009:0001)	Vulnerability - level 4	Vuln
117183	CentOS Security Update for kernel (CESA-2008:0973)	Vulnerability - level 4	Vuln
117186	CentOS Security Update for xterm (CESA-2009:0018)	Vulnerability - level 4	Vuln
117187	CentOS Security Update for SquirrelMail (CESA-2009:0010)	Vulnerability - level 3	Vuln
117204	CentOS Security Update for enscript (CESA-2008:1021)	Vulnerability - level 3	Vuln
117208	CentOS Security Update for enscript (CESA-2008:1016)	Vulnerability - level 3	Vuln
117215	CentOS Security Update for httpd (CESA-2008:0967)	Vulnerability - level 3	Vuln
117231	CentOS Security Update for pam_krb5 (CESA-2008:0907)	Vulnerability - level 3	Vuln
117246	CentOS Security Update for kernel (CESA-2008:0612)	Vulnerability - level 4	Vuln
117257	CentOS Security Update for SeaMonkey (CESA-2008:0547)	Vulnerability - level 5	Vuln
117258	CentOS Security Update for Firefox (CESA-2008:0549)	Vulnerability - level 5	Vuln
117260	CentOS Security Update for Firefox (CESA-2008:0569)	Vulnerability - level 5	Vuln
117262	CentOS Security Update for Pidgin (CESA-2008:0584)	Vulnerability - level 4	Vuln
117267	CentOS Security Update for PHP (CESA-2008:0544)	Vulnerability - level 3	Vuln
117268	CentOS Security Update for PHP (CESA-2008:0545)	Vulnerability - level 3	Vuln
117272	CentOS Security Update for PHP (CESA-2008:0546)	Vulnerability - level 3	Vuln
117273	CentOS Security Update for kernel (CESA-2008:0607)	Vulnerability - level 4	Vuln
117274	CentOS Security Update for Thunderbird (CESA-2008:0616)	Vulnerability - level 3	Vuln
117289	Red Hat Update for OpenSSL (RHSA-2010:0162, RHSA-2010:0163)	Vulnerability - level 3	Vuln
117294	CentOS Security Update for FreeType (CESA-2008:0556)	Vulnerability - level 4	Vuln
117295	CentOS Security Update for FreeType (CESA-2008:0558)	Vulnerability - level 4	Vuln
117307	CentOS Security Update for Kernel (CESA-2008:0237)	Vulnerability - level 4	Vuln
117311	CentOS Security Update for Kernel (CESA-2008:0275)	Vulnerability - level 4	Vuln
117331	Apple Mac OS X Security Update 2010-002 Not Installed (APPLE-SA-2010-03-29-1)	Vulnerability - level 5	Vuln
117339	CentOS Security Update for krb5 (CESA-2008:0181)	Vulnerability - level 5	Vuln
117340	CentOS Security Update for unzip (CESA-2008:0196)	Vulnerability - level 3	Vuln
117343	CentOS Security Update for Tomcat (CESA-2008:0042)	Vulnerability - level 3	Vuln
117344	CentOS Security Update for krb5 (CESA-2008:0164)	Vulnerability - level 5	Vuln
117345	CentOS Security Update for krb5 (CESA-2008:0180)	Vulnerability - level 5	Vuln
117354	CentOS Security Update for tcltk (CESA-2008:0134)	Vulnerability - level 3	Vuln
117355	CentOS Security Update for Tk (CESA-2008:0135)	Vulnerability - level 3	Vuln
117356	CentOS Security Update for Tk (CESA-2008:0136)	Vulnerability - level 3	Vuln

117397	CentOS Security Update for Perl (CESA-2007:0966)	Vulnerability - level 4	Vuln
117412	CentOS Security Update for OpenSSL (CESA-2007:1003)	Vulnerability - level 3	Vuln
117417	CentOS Security Update for Samba (CESA-2007:1016)	Vulnerability - level 5	Vuln
117420	CentOS Security Update for net (CESA-2007:1045)	Vulnerability - level 3	Vuln
117421	CentOS Security Update for util (CESA-2007:0969)	Vulnerability - level 3	Vuln
117422	CentOS Security Update for Samba (CESA-2007:1013)	Vulnerability - level 5	Vuln
117433	Apple QuickTime Multiple Arbitrary Code Execution Vulnerabilities(HT4104)	Vulnerability - level 5	Vuln
117435	Oracle Java SE Critical Patch Update - March 2010	Vulnerability - level 3	Vuln
117436	Mozilla Firefox, SeaMonkey, Thunderbird Multiple Vulnerabilities (MFSA 2010-18, MFSA 2010-19, MFSA 2010-20, MFSA 2010-21, MFSA 2010-16, MFSA 2010-17)	Vulnerability - level 3	Vuln
117438	CentOS Security Update for OpenSSL096b (CESA-2010:0173)	Vulnerability - level 4	Vuln
117439	CentOS Security Update for Thunderbird (CESA-2010:0153)	Vulnerability - level 3	Vuln
117441	CentOS Security Update for OpenSSL (CESA-2010:0162)	Vulnerability - level 4	Vuln
117451	CentOS Security Update for OpenSSL (CESA-2007:0964)	Vulnerability - level 4	Vuln
117455	CentOS Security Update for OpenSSL (CESA-2007:0813)	Vulnerability - level 3	Vuln
117463	CentOS Security Update for cyrus (CESA-2007:0878)	Vulnerability - level 3	Vuln
117464	CentOS Security Update for cyrus (CESA-2007:0795)	Vulnerability - level 3	Vuln
117466	CentOS Security Update for krb5 (CESA-2007:0858)	Vulnerability - level 4	Vuln
117479	CentOS Security Update for Tomcat (CESA-2007:0569)	Vulnerability - level 3	Vuln
11748	PHPNews SQL Injection Vulnerability	Potential Vulnerability - level 4	
11748	WAGO PLC Ethernet Web-based Management Authentication Bypass Vulnerability	Potential Vulnerability - level 4	Practice
117514	CentOS Security Update for gcc (CESA-2007:0473)	Vulnerability - level 3	Vuln
117539	CentOS Security Update for gcc (CESA-2007:0220)	Vulnerability - level 3	Vuln
117550	CentOS Security Update for unzip (CESA-2007:0203)	Vulnerability - level 2	Vuln
117561	CentOS Security Update for Tomcat (CESA-2007:0327)	Vulnerability - level 4	Vuln
117598	CentOS Security Update for Samba (CESA-2007:0060)	Vulnerability - level 3	Vuln
11761	Mozilla Camino Web Browser Infinite Array Sort Denial Of Service Vulnerability	Potential Vulnerability - level 3	
11761	Splunk Enterprise OpenSSL Multiple Vulnerabilities (SP-CAAN4P)	Potential Vulnerability - level 3	Practice
117623	CentOS Security Update for Texinfo (CESA-2006:0727)	Vulnerability - level 3	Vuln
117634	CentOS Security Update for OpenSSH (CESA-2006:0698)	Vulnerability - level 4	Vuln
117646	Solaris BIND Software DNS Cache Poisoning Vulnerability (1021660.1)	Vulnerability - level 2	Vuln
117666	CentOS Security Update for OpenSSH (CESA-2006:0298)	Vulnerability - level 2	Vuln
117667	CentOS Security Update for elfutils (CESA-2006:0368)	Vulnerability - level 2	Vuln
117681	CentOS Security Update for elfutils (CESA-2006:0354)	Vulnerability - level 2	Vuln
117722	CentOS Security Update for Firefox (CESA-2006:0328)	Vulnerability - level 5	Vuln
117723	CentOS Security Update for Mozilla (CESA-2006:0329)	Vulnerability - level 5	Vuln
117725	CentOS Security Update for Thunderbird (CESA-2006:0330)	Vulnerability - level 5	Vuln
117732	CentOS Security Update for Kernel (CESA-2006:0132)	Vulnerability - level 3	Vuln
117733	CentOS Security Update for Python (CESA-2006:0197)	Vulnerability - level 3	Vuln
117739	CentOS Security Update for GnuPG (CESA-2006:0266)	Vulnerability - level 4	Vuln
117753	CentOS Security Update for GNU TLS (CESA-2006:0207)	Vulnerability - level 4	Vuln
117754	CentOS Security Update for xpdf (CESA-2006:0201)	Vulnerability - level 4	Vuln
117756	CentOS Security Update for kdegraphics (CESA-2006:0206)	Vulnerability - level 4	Vuln
117770	CentOS Security Update for kdelibs (CESA-2006:0184)	Vulnerability - level 5	Vuln
117774	VMware Hosted Products, vCenter Server and ESX Multiple Security Issues (VMSA-2010-0007)	Vulnerability - level 4	Vuln
117784	CentOS Security Update for cURL (CESA-2005:875)	Vulnerability - level 3	Vuln
117789	CentOS Security Update for cURL (CESA-2005:807)	Vulnerability - level 3	Vuln
117790	CentOS Security Update for Wget (CESA-2005:812)	Vulnerability - level 4	Vuln
117807	CentOS Security Update for Binutils (CESA-2005:673)	Vulnerability - level 2	Vuln
117810	CentOS Security Update for GDB (CESA-2005:709)	Vulnerability - level 2	Vuln
117816	CentOS Security Update for Binutils (CESA-2005:763)	Vulnerability - level 2	Vuln

117828	CentOS Security Update for GDB (CESA-2005:801)	Vulnerability - level 2	Vuln
117833	CentOS Security Update for httpd (CESA-2005:608)	Vulnerability - level 4	Vuln
117835	CentOS Security Update for PCRE (CESA-2005:761)	Vulnerability - level 3	Vuln
117836	CentOS Security Update for Exim (CESA-2005:358)	Vulnerability - level 3	Vuln
117850	CentOS Security Update for Binutils (CESA-2005:659)	Vulnerability - level 2	Vuln
117863	Red Hat Update for krb5 (RHSA-2010:0343)	Vulnerability - level 3	Vuln
11787	Advantech WebAccess Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
11787	gnubiff Multiple Remote Denial Of Service Vulnerabilities	Vulnerability - level 3	
117879	CentOS Security Update for Zlib (CESA-2005:569)	Vulnerability - level 4	Vuln
117886	CentOS Security Update for Zlib (CESA-2005:584)	Vulnerability - level 4	Vuln
117891	CentOS Security Update for httpd (CESA-2005:582)	Vulnerability - level 3	Vuln
117907	Red Hat Update for kdebse (RHSA-2010:0348)	Vulnerability - level 3	Vuln
117976	CentOS Security Update for cURL (CESA-2010:0329)	Vulnerability - level 3	Vuln
117977	CentOS Security Update for SeaMonkey (CESA-2010:0333)	Vulnerability - level 5	Vuln
117978	CentOS Security Update for Firefox (CESA-2010:0332)	Vulnerability - level 5	Vuln
117979	Red Hat cURL Security Update (RHSA-2010:0329)	Vulnerability - level 3	Vuln
118010	Internet Download Manager FTP Buffer Overflow Vulnerability	Vulnerability - level 3	Vuln
118013	CentOS Security Update for kdebse (CESA-2010:0348)	Vulnerability - level 4	Vuln
118025	Red Hat Update for Kernel (RHSA-2010:0398)	Vulnerability - level 3	Vuln
118026	Red Hat Security Update for teTeX (RHSA-2010:0400)	Vulnerability - level 3	Vuln
118034	Free Download Manager Multiple Vulnerabilities	Vulnerability - level 3	Vuln
118038	Fetchmail Debug Mode POP3 UIDL Lists Denial of Service Vulnerability	Vulnerability - level 1	Vuln
118040	Java for Mac OS X 10.6 Update 2 and Java for Mac OS X 10.5 Update 7 (APPLE-SA-2010-05-18-1, APPLE-SA-2010-05-18-2)	Vulnerability - level 4	Vuln
118041	Aria2 Metalink "name" Directory Traversal Vulnerability	Vulnerability - level 3	Vuln
118045	Red Hat Update for krb5 (RHSA-2010:0423)	Vulnerability - level 3	Vuln
118048	CentOS Security Update for kernel (CESA-2010:0394)	Vulnerability - level 4	Vuln
118050	CentOS Security Update for teTeX (CESA-2010:0399)	Vulnerability - level 3	Vuln
118058	IBM AIX OpenSSL Denial of Service Vulnerability	Vulnerability - level 3	Vuln
11806	Apache Hadoop Prior to 2.7.0 Multiple Vulnerabilities	Vulnerability - level 3	Vuln
118072	VMware ESX Service Console Third Party Updates (VMSA-2010-0009)	Vulnerability - level 4	Vuln
118078	HP-UX Running Java multiple Vulnerabilities (HPSBUX02524)	Vulnerability - level 3	Vuln
118079	HP-UX Running Apache-Based Web Server Remote Denial of Service Vulnerability (HPSBUX02531)	Vulnerability - level 3	Vuln
118090	Apple Safari Multiple Vulnerabilities (HT4196)	Vulnerability - level 4	Vuln
118097	CA (Computer Associates) PSFormX and WebScan ActiveX Controls Multiple Vulnerabilities (CA20100608-01)	Vulnerability - level 3	Vuln
118106	Apple Mac OS X Security Update 2010-004 Not Installed (APPLE-SA-2010-06-15-1)	Vulnerability - level 5	Vuln
118109	Apple iTunes Multiple Vulnerabilities (HT4220)	Vulnerability - level 4	Vuln
118110	HP-UX Running Tomcat Servlet Engine Remote Privilege Escalation Vulnerability (HPSBUX02541)	Vulnerability - level 3	Vuln
11812	Advantech WebAccess Stack-Based Buffer Overflow Vulnerability	Vulnerability - level 3	Vuln
118122	CentOS Security Update for krb5 (CESA-2010:0423)	Vulnerability - level 4	Vuln
118130	CentOS Security Update for teTeX (CESA-2010:0400)	Vulnerability - level 3	Vuln
118131	CentOS Security Update for Kernel (CESA-2010:0398)	Vulnerability - level 4	Vuln
118132	CentOS Security Update for krb5 (CESA-2010:0343)	Vulnerability - level 4	Vuln
118148	HP-UX Running Kerberos Remote Denial of Service Vulnerability (HPSBUX02544)	Vulnerability - level 3	Vuln
118150	CentOS Security Update for Java (CESA-2010:0339)	Vulnerability - level 4	Vuln
118190	Multiple Vendor Info-ZIP Unzip 5.52 Command File Creation Vulnerability	Vulnerability - level 2	Vuln
118192	Fedora Update for Bournal (FEDORA-2010-3168)	Vulnerability - level 2	Vuln
118200	Fedora Update for fcron (FEDORA-2010-4084)	Vulnerability - level 1	Vuln
118209	Winamp VP6 Content Parsing Buffer Overflow Vulnerability	Vulnerability - level 3	Vuln
118221	Fedora Update for Galeon, Miro, Gnome, Perl, Mozvoikko, Firefox, Xulrunner (FEDORA-2010-5202)	Vulnerability - level 5	Vuln

118222	Fedora Update for Thunderbird, Sunbird (FEDORA-2010-5561)	Vulnerability - level 5	Vuln
118226	Fedora Update for OpenSSL (FEDORA-2010-5744)	Vulnerability - level 5	Vuln
118227	Fedora Update for ViewVC (FEDORA-2010-5805)	Vulnerability - level 3	Vuln
118233	CentOS Security Update for Kernel (CESA-2010:0504)	Vulnerability - level 4	Vuln
118250	Fedora Update for SeaMonkey (FEDORA-2010-6236)	Vulnerability - level 5	Vuln
118251	Fedora Update for Java (FEDORA-2010-6279)	Vulnerability - level 4	Vuln
118255	Fedora Update for kdbase-workspace (FEDORA-2010-6605)	Vulnerability - level 3	Vuln
118275	Solaris Unzip Multiple Vulnerabilities	Vulnerability - level 3	Vuln
118287	Fedora Update for KDE SC (FEDORA-2010-8577)	Vulnerability - level 3	Vuln
118290	Fedora Update for krb (FEDORA-2010-8749)	Vulnerability - level 3	Vuln
118291	Fedora Update for aria (FEDORA-2010-8905)	Vulnerability - level 2	Vuln
118303	Linux Kernel CIFS DNS Lookup Keyring Cache Poisoning Vulnerability	Vulnerability - level 2	Vuln
118327	Apple Mac OS X WebDAV Kernel Extension Local Denial of Service Vulnerability	Vulnerability - level 2	Vuln
118330	CentOS Security Update for libtiff (CESA-2010:0519)	Vulnerability - level 4	Vuln
118337	CentOS Security Update for Thunderbird (CESA-2010:0545)	Vulnerability - level 5	Vuln
118362	Fedora Update for RPM (FEDORA-2010-9829)	Vulnerability - level 4	Vuln
118377	FreeType Compact Font Format (CFF) Multiple Stack Based Buffer Overflow Vulnerabilities	Vulnerability - level 3	Vuln
118387	Opera Web Browser Multiple Vulnerabilities	Vulnerability - level 3	Vuln
118429	Fedora Update for Java (FEDORA-2010-6025)	Vulnerability - level 4	Vuln
118430	Fedora Update for Java (FEDORA-2009-8329,FEDORA-2009-8337)	Vulnerability - level 4	Vuln
118431	Fedora Update for Java (FEDORA-2010-6039)	Vulnerability - level 4	Vuln
118432	Adobe Shockwave Player Remote Code Execution Vulnerabilities (APSB10-20)	Vulnerability - level 4	Vuln
118442	RealPlayer Update for Multiple Vulnerabilities	Vulnerability - level 3	Vuln
118452	VMware ESX 3.X Third Party Updates for Service Console (VMSA-2010-0013)	Vulnerability - level 3	Vuln
118454	CentOS Security Update for Tomcat5 (CESA-2010:0580)	Vulnerability - level 4	Vuln
118460	CentOS Security Update for Thunderbird (CESA-2010:0544)	Vulnerability - level 3	Vuln
118461	CentOS Security Update for Kernel (CESA-2010:0610)	Vulnerability - level 4	Vuln
118464	CentOS Security Update for libtiff (CESA-2010:0520)	Vulnerability - level 4	Vuln
118475	CentOS Security Update for Kernel (CESA-2010:0606)	Vulnerability - level 4	Vuln
118478	CentOS Security Update for HTTP (CESA-2010:0659)	Vulnerability - level 3	Vuln
118489	MailEnable SMTP Service Two Denial of Service Vulnerabilities	Potential Vulnerability - level 3	Practice
118504	Fedora Update for SBLIM SFCB (FEDORA-2010-10323)	Vulnerability - level 5	Vuln
118506	Fedora Update for LibTIFF (FEDORA-2010-10334)	Vulnerability - level 4	Vuln
118507	HP-UX Running BIND Remote Denial of Service Vulnerability (HPSBUX02546)	Vulnerability - level 3	Vuln
118512	Fedora Update for gcc (FEDORA-2010-10415)	Vulnerability - level 3	Vuln
118513	Fedora Update for mingw (FEDORA-2010-10460)	Vulnerability - level 3	Vuln
118514	Fedora Update for KVIrc (FEDORA-2010-10522)	Vulnerability - level 5	Vuln
118541	CentOS Security Update for RPM (CESA-2010:0678)	Vulnerability - level 3	Vuln
118544	CentOS Security Update for RPM (CESA-2010:0679)	Vulnerability - level 3	Vuln
118548	CentOS Security Update for bzip2 (CESA-2010:0703)	Vulnerability - level 4	Vuln
118553	Solaris GSS-API NULL Pointer Dereference Vulnerability	Vulnerability - level 2	Vuln
118561	Solaris FreeType Buffer Overflow Vulnerability	Vulnerability - level 3	Vuln
118569	VMware ESX Third Party Updates for Service Console (VMSA-2010-0015)	Vulnerability - level 3	Vuln
118589	Red Hat Update for Kernel (RHSA-2010:0723)	Vulnerability - level 4	Vuln
118590	Red Hat Update for MikMod (RHSA-2010:0720)	Vulnerability - level 2	Vuln
118591	Red Hat Update for bzip2 (RHSA-2010:0703)	Vulnerability - level 3	Vuln
118597	Oracle Java SE Critical Patch Update - October 2010	Vulnerability - level 4	Vuln
11860	Advantech WebAccess Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
11860	PunBB Post Count Modification Vulnerability	Vulnerability - level 3	
118616	Solaris libtiff Integer Overflow and Denial of Service Vulnerabilities	Vulnerability - level 3	Vuln

118617	Solaris Tomcat Multiple Vulnerabilities	Vulnerability - level 3	Vuln
118618	CentOS Security Update for MikMod (CESA-2010:0720)	Vulnerability - level 3	Vuln
118620	CentOS Security Update for Kernel (CESA-2010:0723)	Vulnerability - level 4	Vuln
118622	Red Hat Update for Java (RHSA-2010:0768)	Vulnerability - level 4	Vuln
118623	Red Hat Update for RPM (RHSA-2010:0679)	Vulnerability - level 3	Vuln
118627	Red Hat Update for httpd (RHSA-2010:0659)	Vulnerability - level 4	Vuln
118632	Java for Mac OS X 10.6 Update 3 and OS X 10.5 Update 8 (APPLE-SA-2010-10-20-1, APPLE-SA-2010-10-20-2)	Vulnerability - level 4	Vuln
118651	CentOS Security Update for Java (CESA-2010:0768)	Vulnerability - level 4	Vuln
118664	Red Hat Update for Kernel (RHSA-2010:0779)	Vulnerability - level 4	Vuln
118681	Red Hat Update for PAM (RHSA-2010:0819)	Vulnerability - level 4	Vuln
118713	Fedora Update for Kernel (FEDORA-2010-11462)	Vulnerability - level 2	Vuln
118718	Fedora Update for ssmtp (FEDORA-2010-11836)	Vulnerability - level 1	Vuln
118727	Red Hat Update for Kernel (RHSA-2010:0839)	Vulnerability - level 4	Vuln
118738	VMware updates for Service Console and Likewise components (VMSA-2010-0016)	Vulnerability - level 3	Vuln
118757	Fedora Update for HTTPD (FEDORA-2010-12478)	Vulnerability - level 3	Vuln
118763	Fedora Update for Kernel (FEDORA-2010-13058)	Vulnerability - level 4	Vuln
118781	Winamp Multiple Vulnerabilities	Vulnerability - level 3	Vuln
118783	Red Hat Update for krb5 (RHSA-2010:0926)	Vulnerability - level 4	Vuln
118785	CentOS Security Update for Kernel (CESA-2010:0779)	Vulnerability - level 3	Vuln
118793	Solaris "bzip2" Integer Overflow Vulnerability	Vulnerability - level 2	Vuln
118794	HP-UX Apache Running Tomcat Servlet Engine Remote Information Disclosure Vulnerability (HPSBUX02579)	Vulnerability - level 3	Vuln
118799	Red Hat Update for Kernel (RHSA-2010:0936)	Vulnerability - level 4	Vuln
118807	VMware ESX Third Party Updates for Service Console (VMSA-2010-0019)	Vulnerability - level 3	Vuln
118810	CentOS Security Update for PAM (CESA-2010:0819)	Vulnerability - level 3	Vuln
118814	CentOS Security Update for Kernel (CESA-2010:0839)	Vulnerability - level 3	Vuln
118819	CentOS Security Update for krb5 (CESA-2010:0926)	Vulnerability - level 3	Vuln
118824	HP-UX Apache-based Web Server Remote Denial of Service Vulnerability (HPSBUX02612)	Vulnerability - level 3	Vuln
118829	HP-UX Running Java Multiple Vulnerabilities (HPSBUX02608)	Vulnerability - level 3	Vuln
118830	Red Hat Update for OpenSSL (RHSA-2010:0978)	Vulnerability - level 4	Vuln
118831	Red Hat Update for BIND (RHSA-2010:0976)	Vulnerability - level 4	Vuln
118832	Red Hat Update for OpenSSL (RHSA-2010:0977)	Vulnerability - level 4	Vuln
118833	Red Hat Update for Kernel (RHSA-2010:0606)	Vulnerability - level 4	Vuln
118843	Red Hat Update for Xulrunner Firefox (RHSA-2010:0112)	Vulnerability - level 5	Vuln
118846	Red Hat Update for Xulrunner Firefox (RHSA-2010:0332)	Vulnerability - level 5	Vuln
118848	Red Hat Update for cURL (RHSA-2010:0273)	Vulnerability - level 4	Vuln
118849	Red Hat Update for pam_krb5 (RHSA-2010:0258)	Vulnerability - level 4	Vuln
118855	Red Hat Update for Java -1.6.0-OpenJDK (RHSA-2010:0339)	Vulnerability - level 4	Vuln
118858	Red Hat Update for Kernel (RHSA-2010:0504)	Vulnerability - level 4	Vuln
118867	Red Hat Update for Tomcat 5 (RHSA-2010:0580)	Vulnerability - level 4	Vuln
118882	CentOS Security Update for BIND (CESA-2010:0976)	Vulnerability - level 4	Vuln
118883	CentOS Security Update for OpenSSL (CESA-2010:0978)	Vulnerability - level 3	Vuln
118888	Microsoft Windows Shell Graphics Processing Remote Code Execution Vulnerability (MS11-006 and KB2490606)	Vulnerability - level 3	Vuln
11889	PhpDig Unspecified Remote Vulnerability	Vulnerability - level 5	
11889	TripWire Enterprise Console Prior to version 8.6.0 Multiple Vulnerabilities.	Vulnerability - level 5	Vuln
118892	Red Hat Update for Kernel (RHSA-2011:0004)	Vulnerability - level 4	Vuln
118912	Red Hat Update for Kernel (RHSA-2011:0017)	Vulnerability - level 4	Vuln
118913	Red Hat Update for Kernel (RHSA-2011:0007)	Vulnerability - level 4	Vuln
118919	Red Hat Update for Kernel (RHSA-2011:0163)	Vulnerability - level 4	Vuln
118940	HP-UX Running Kerberos Remote Unauthorized Modification Vulnerability (HPSBUX02623)	Vulnerability - level 3	Vuln
118942	Red Hat Update for Kernel (RHSA-2011:0162)	Vulnerability - level 3	Vuln

11895	Advantech/BroadWin WebAccess Multiple Vulnerabilities	Potential Vulnerability - level 5	Practice
11895	mnoGoSearch Multiple Cross-Site Scripting Vulnerabilities	Potential Vulnerability - level 5	
118961	Solaris Apache 2.0.x HTTP Server mod_dav Denial of Service Vulnerability	Vulnerability - level 3	Vuln
118963	Red Hat Update for Java -1.5.0-ibm (RHSA-2011:0169)	Vulnerability - level 5	Vuln
118964	Red Hat Update for Java -1.4.2-ibm (RHSA-2011:0152)	Vulnerability - level 4	Vuln
118965	Red Hat Update for Java -1.6.0-Sun (RHSA-2010:0770)	Vulnerability - level 5	Vuln
118967	VMware ESX Security Update for Third-Party Components (VMSA-2011-0003)	Vulnerability - level 3	Vuln
118969	Red Hat Update for java-1.6.0-ibm (RHSA-2010:0987)	Vulnerability - level 5	Vuln
118977	Red Hat Update for krb5 (RHSA-2011:0199)	Vulnerability - level 3	Vuln
118978	Red Hat Update for krb5 (RHSA-2011:0200)	Vulnerability - level 3	Vuln
118984	Red Hat Update for Kernel (RHSA-2011:0263)	Vulnerability - level 4	Vuln
118996	CentOS Security Update for Kernel (CESA-2011:0004)	Vulnerability - level 4	Vuln
118997	CentOS Security Update for Kernel (CESA-2010:0936)	Vulnerability - level 4	Vuln
119003	CentOS Security Update for OpenSSL (CESA-2010:0977)	Vulnerability - level 3	Vuln
119005	CentOS Security Update for BIND (CESA-2010:1000)	Vulnerability - level 4	Vuln
119008	CentOS Security Update for Kernel (CESA-2011:0162)	Vulnerability - level 4	Vuln
119019	Solaris Kerberos Input Validation Vulnerability	Vulnerability - level 3	Vuln
119031	VMware ESX SLPD Denial of Service Vulnerability and Security Update for Third-Party Components (VMSA-2011-0004)	Vulnerability - level 3	Vuln
119037	Red Hat Update for Kernel (RHSA-2011:0303)	Vulnerability - level 4	Vuln
119040	Red Hat Update for Tomcat 6 (RHSA-2011:0335)	Vulnerability - level 3	Vuln
119057	HP-UX Running OpenSSL Multiple Vulnerabilities (HPSBUX02638)	Vulnerability - level 3	Vuln
119060	Solaris "bzip2" Integer Overflow Vulnerability	Vulnerability - level 3	Vuln
119064	Apple Mac OS X v10.6.7 and Security Update 2011-001 Not Installed (APPLE-SA-2011-03-21-1)	Vulnerability - level 4	Vuln
11907	Advantech WebAccess Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
11907	PhpGedView Calendar.PHP Cross-Site Scripting Vulnerability	Vulnerability - level 3	
119081	Red Hat Update for libtiff (RHSA-2011:0392)	Vulnerability - level 4	Vuln
119085	Solaris BIND DNS Software Multiple Vulnerabilities	Vulnerability - level 3	Vuln
119096	Red Hat Update for Firefox (RHSA-2008:0569)	Vulnerability - level 5	Vuln
11910	Cloudera Manager Information Disclosure Vulnerability.	Vulnerability - level 4	Vuln
11910	PhpGedView Placelist.PHP SQL Injection Vulnerability	Vulnerability - level 4	
119101	Red Hat Update for krb5 (RHSA-2008:0164)	Vulnerability - level 5	Vuln
119122	VMware Multiple Product Vmrun Utility Privilege Escalation Vulnerability (VMSA-2011-0006)	Vulnerability - level 3	Vuln
119131	Red Hat Update for glibc (RHSA-2011:0412)	Vulnerability - level 4	Vuln
119138	Red Hat Update for Kernel (RHSA-2011:0421)	Vulnerability - level 4	Vuln
119146	Red Hat Update for kernel (RHSA-2011:0429)	Vulnerability - level 4	Vuln
119155	RealPlayer Predictable Temporary Filename Code Execution Vulnerability	Vulnerability - level 3	Vuln
119157	HP-UX Running BIND Remote Denial of Service Vulnerability (HPSBUX02655)	Vulnerability - level 3	Vuln
119177	Solaris Kerberos Design Error Vulnerability	Vulnerability - level 2	Vuln
119179	Solaris Kerberos Multiple Vulnerabilities	Vulnerability - level 3	Vuln
119186	HP-UX Running Java multiple Vulnerabilities (HPSBUX02805)	Vulnerability - level 4	Vuln
119191	CentOS Security Update for Kernel (CESA-2011:0429)	Vulnerability - level 4	Vuln
119193	CentOS Security Update for glibc (CESA-2011:0412)	Vulnerability - level 4	Vuln
119202	CentOS Security Update for Kernel (CESA-2011:0163)	Vulnerability - level 4	Vuln
119203	CentOS Security Update for Kernel (CESA-2011:0303)	Vulnerability - level 3	Vuln
119204	CentOS Security Update for krb5 (CESA-2011:0199)	Vulnerability - level 4	Vuln
119205	CentOS Security Update for libtiff (CESA-2011:0392)	Vulnerability - level 4	Vuln
11921	Cloudera CDH Remote Code Execution Vulnerability.	Vulnerability - level 5	Vuln
11921	Linux Kernel SCM_SEND Local Denial of Service Vulnerability	Vulnerability - level 5	
119216	VMware ESX Denial of Service and ESX Service Console (VMSA-2011-0007)	Vulnerability - level 3	Vuln

119227	Solaris OpenSSL Unauthorized Modification Vulnerability	Vulnerability - level 3	Vuln
119233	Solaris Apache 2 HTTP Server Multiple Vulnerabilities	Vulnerability - level 5	Vuln
119256	Adobe Flash Media Server Security Update (APSB11-11)	Vulnerability - level 4	Vuln
11926	Gemalto HASP SRM, Sentinel HASP and Sentinel LDK hasplms Service Multiple Security Vulnerabilities	Vulnerability - level 4	Vuln
11926	Roxio Toast TDIxSupport Local Format String Vulnerability	Vulnerability - level 4	
11927	Gemalto HASP SRM, Sentinel HASP and Sentinel LDK hasplms Service Dos Vulnerability	Vulnerability - level 4	Vuln
11927	Microsoft Word for Windows 6.0 Converter Table Conversion Buffer Overflow Vulnerability	Vulnerability - level 4	
119274	Red Hat Update for Tomcat6 (RHSA-2011:0791)	Vulnerability - level 3	Vuln
119281	Red Hat Update for Red Hat Enterprise Linux 6.1 Kernel (RHSA-2011:0542)	Vulnerability - level 4	Vuln
119297	Red Hat Update for Kernel (RHSA-2011:0833)	Vulnerability - level 4	Vuln
119300	Red Hat Update for Postfix (RHSA-2011:0843)	Vulnerability - level 3	Vuln
119302	Red Hat Update for GIMP (RHSA-2011:0837)	Vulnerability - level 3	Vuln
119303	Red Hat Update for GIMP (RHSA-2011:0838)	Vulnerability - level 3	Vuln
119341	RealNetworks RealPlayer Multiple Vulnerabilities	Vulnerability - level 4	Vuln
119352	Apple Mac OS X v10.6.8 and Security Update 2011-004 Not Installed (APPLE-SA-2011-06-23-1)	Vulnerability - level 4	Vuln
119381	Red Hat Update for krb5-appl (RHSA-2011:0920)	Vulnerability - level 4	Vuln
119399	CentOS Security Update for Postfix (CESA-2011:0843)	Vulnerability - level 3	Vuln
119400	CentOS Security Update for GIMP (CESA-2011:0838)	Vulnerability - level 3	Vuln
119403	CentOS Security Update for Kernel (CESA-2011:0833)	Vulnerability - level 4	Vuln
119412	IBM AIX BIND Denial of Service Vulnerability	Vulnerability - level 3	Vuln
119414	CentOS Security Update for GIMP (CESA-2011:0837)	Vulnerability - level 3	Vuln
119452	Novell Vibe OnPrem Apache Tomcat Denial of Service Vulnerability	Vulnerability - level 3	Vuln
119463	FreeRADIUS OSCP Authentication Bypass Vulnerability	Vulnerability - level 3	Vuln
119484	CA Gateway Security URL Parsing Vulnerability	Vulnerability - level 4	Vuln
119502	ISC DHCP Denial of Service Vulnerabilities (Deprecated)	Vulnerability - level 3	Vuln
119505	BlackBerry Enterprise Server PNG and TIFF Image Processing Vulnerabilities	Vulnerability - level 4	Vuln
119506	Novell eDirectory OpenSSL Ciphersuite Downgrade Vulnerability	Vulnerability - level 2	Vuln
119507	Red Hat Update for DHCP (RHSA-2011:1160)	Vulnerability - level 3	Vuln
119559	CentOS Security Update for DHCP (CESA-2011:1160)	Vulnerability - level 3	Vuln
119591	InduSoft ISSymbol ActiveX Control "ISSymbol.ocx" Multiple Buffer Overflow Vulnerabilities	Vulnerability - level 4	Vuln
119638	Apple Mac OS X Lion v10.7.2 and Security Update 2011-006 Not Installed (APPLE-SA-2011-10-12-3)	Vulnerability - level 4	Vuln
119701	VMware ESX Updates to Third Party Libraries and ESX Service Console (VMSA-2011-0012)	Vulnerability - level 3	Vuln
119709	Multiple Schneider Electric Products UnitelWay Device Driver Privilege Escalation Vulnerability	Vulnerability - level 4	Vuln
119732	IBM AIX OpenSSL Multiple Vulnerabilities	Vulnerability - level 3	Vuln
119742	Solaris Apache Tomcat Multiple Vulnerabilities	Vulnerability - level 3	Vuln
119745	HP Directories Support for ProLiant Management Processors Unauthorized Access Security Bypass	Vulnerability - level 3	Vuln
119749	VMware Third Party Component Updates for VMware vCenter Server, vCenter Update Manager (VMSA-2011-0013)	Vulnerability - level 3	Vuln
119756	HP-UX Apache Running Tomcat Servlet Engine Multiple Vulnerabilities (HPSBUX02725)	Vulnerability - level 3	Vuln
119759	Red Hat Update for Kernel (RHSA-2011:1465)	Vulnerability - level 4	Vuln
119830	Red Hat Update for Tomcat5 (RHSA-2011:1845)	Vulnerability - level 3	Vuln
119837	7-Technologies Interactive Graphical SCADA System Buffer Overflow Vulnerability	Potential Vulnerability - level 4	Practice
119886	Red Hat Update for t1lib (RHSA-2012:0062)	Vulnerability - level 3	Vuln
119900	F5 Big-IP Multiple Code Execution Vulnerabilities (SOL11853)	Vulnerability - level 4	Vuln
119903	VMware ESX Server Multiple Vulnerabilities (VMSA-2012-0001)	Vulnerability - level 4	Vuln

119904	F5 Big-IP Multiple BIND Vulnerabilities (SOL12729, SOL12778, SOL12816)	Vulnerability - level 3	Vuln
119914	Solaris Apache Tomcat Multiple Vulnerabilities	Vulnerability - level 3	Vuln
119919	Apple Mac OS X Lion v10.7.3 and Security Update 2012-001 Not Installed (APPLE-SA-2012-02-01-1)	Vulnerability - level 5	Vuln
119935	Novell iPrint Client Multiple Remote Code Execution Vulnerabilities	Vulnerability - level 4	Vuln
119949	Red Hat Update for TeX Live (RHSA-2012:0137)	Vulnerability - level 3	Vuln
11995	Advantech WebAccess Multiple Security Vulnerabilities	Vulnerability - level 4	Vuln
11995	Convex 3D Buffer Overflow Vulnerability	Vulnerability - level 4	
119968	RealPlayer Multiple Remote Code Execution Vulnerabilities	Vulnerability - level 5	Vuln
119990	Red Hat Update for krb5 (RHSA-2012:0306)	Vulnerability - level 2	Vuln
120003	Solaris "libtiff" Integer Overflow and Denial of Service	Vulnerability - level 3	Vuln
120004	Solaris BIND DNS Software Multiple Vulnerabilities	Vulnerability - level 3	Vuln
120023	CentOS Security Update for t1lib (CESA-2012:0062)	Vulnerability - level 4	Vuln
120049	CentOS Security Update for TeX Live (CESA-2012:0137)	Vulnerability - level 4	Vuln
120064	Red Hat Update for OpenOffice.org (RHSA-2012:0411)	Vulnerability - level 4	Vuln
120065	Red Hat Update for Raptor (RHSA-2012:0410)	Vulnerability - level 4	Vuln
120068	IntegraXor Project ActiveX Control Insecure Method	Vulnerability - level 3	Vuln
120077	VMware ESXi 3.5 Several Security Vulnerabilities (VMSA-2012-0006)	Vulnerability - level 4	Vuln
120087	CentOS Security Update for Raptor (CESA-2012:0410)	Vulnerability - level 3	Vuln
120088	CentOS Security Update for OpenOffice.org (CESA-2012:0411)	Vulnerability - level 3	Vuln
120129	Solaris Multiple Vulnerabilities in LibTIFF	Vulnerability - level 4	Vuln
120213	Adobe Shockwave Player Multiple Vulnerabilities (APSB12-13)	Vulnerability - level 4	Vuln
120215	KingSCADA Insecure Password Encryption Information Disclosure Vulnerability	Vulnerability - level 3	Vuln
120219	Apple Mac OS X Lion v10.7.4 and Security Update 2012-002 Not Installed (APPLE-SA-2012-05-09-1)	Vulnerability - level 5	Vuln
120221	Apple QuickTime Prior to 7.7.2 Multiple Vulnerabilities (APPLE-SA-2012-05-15-1)	Vulnerability - level 4	Vuln
120230	OpenOffice.org Two Vulnerabilities	Vulnerability - level 4	Vuln
120270	Red Hat Update for OpenOffice.org (RHSA-2012:0705)	Vulnerability - level 4	Vuln
120273	Java for OS X 2012-004 and Java for Mac OS X 10.6 Update 9 (APPLE-SA-2012-06-12-1)	Vulnerability - level 5	Vuln
120274	Oracle Java SE Critical Patch Update - June 2012	Vulnerability - level 5	Vuln
120287	Red Hat Update for java-1.6.0-sun (RHSA-2012:0734)	Vulnerability - level 5	Vuln
120296	Cisco AnyConnect Secure Mobility Client Multiple Vulnerabilities	Vulnerability - level 3	Vuln
120297	Google Chrome Prior to 20.0.1132.43 Multiple Vulnerabilities	Vulnerability - level 4	Vuln
120325	Red Hat Update for java-1.7.0-oracle (RHSA-2012:1019)	Vulnerability - level 5	Vuln
120369	Red Hat Update for glibc (RHSA-2012:1097)	Vulnerability - level 3	Vuln
120370	Red Hat Update for glibc (RHSA-2012:1098)	Vulnerability - level 3	Vuln
120381	Red Hat Update for OpenOffice.org (RHSA-2012:1136)	Vulnerability - level 4	Vuln
120382	Red Hat Update for LibreOffice (RHSA-2012:1135)	Vulnerability - level 4	Vuln
120415	CentOS Security Update for OpenOffice.org (CESA-2012:0705)	Vulnerability - level 4	Vuln
120436	Red Hat Update for GIMP (RHSA-2012:1181)	Vulnerability - level 3	Vuln
120439	Red Hat Update for teTeX (RHSA-2012:1201)	Vulnerability - level 3	Vuln
120443	Oracle Java Runtime Environment Remote Code Execution Vulnerability	Vulnerability - level 4	Vuln
120451	Mozilla Firefox/Thunderbird/SeaMonkey Multiple Vulnerabilities (MFSA 2012-57 through MFSA 2012-73)	Vulnerability - level 4	Vuln
120452	Red Hat Update for Thunderbird (RHSA-2012:1211)	Vulnerability - level 5	Vuln
120453	Red Hat Update for Xulrunner Firefox (RHSA-2012:1210)	Vulnerability - level 5	Vuln
120488	CentOS Security Update for glibc (CESA-2012:1097)	Vulnerability - level 3	Vuln
120489	CentOS Security Update for glibc (CESA-2012:1098)	Vulnerability - level 3	Vuln
120505	Red Hat Update for java-1.6.0-openjdk (RHSA-2012:1222)	Vulnerability - level 4	Vuln
120506	Red Hat Update for java-1.7.0-openjdk (RHSA-2012:1223)	Vulnerability - level 4	Vuln
120507	Red Hat Update for java-1.6.0-openjdk (RHSA-2012:1221)	Vulnerability - level 5	Vuln
120508	Red Hat Update for java-1.7.0-oracle (RHSA-2012:1225)	Vulnerability - level 5	Vuln

120511	Red Hat Update for java-1.6.0-ibm (RHSA-2012:1238)	Vulnerability - level 5	Vuln
120515	Red Hat Update for libexif (RHSA-2012:1255)	Vulnerability - level 3	Vuln
120521	Red Hat Update for libxslt (RHSA-2012:1265)	Vulnerability - level 4	Vuln
120528	Red Hat Update for java-1.7.0-ibm (RHSA-2012:1289)	Vulnerability - level 5	Vuln
120531	Apple Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004 Not Installed (APPLE-SA-2012-09-19-2)	Vulnerability - level 4	Vuln
120536	Solaris Multiple Vulnerabilities in Oracle Java Web Console	Vulnerability - level 3	Vuln
120555	Red Hat Update for Kernel (RHSA-2012:1323)	Vulnerability - level 4	Vuln
120556	Red Hat Update for FreeRADIUS (RHSA-2012:1326)	Vulnerability - level 3	Vuln
120557	Red Hat Update for freeradius2 (RHSA-2012:1327)	Vulnerability - level 3	Vuln
120562	CentOS Security Update for OpenOffice.org (CESA-2012:1136)	Vulnerability - level 4	Vuln
120563	CentOS Security Update for LibreOffice (CESA-2012:1135)	Vulnerability - level 4	Vuln
120570	CentOS Security Update for GIMP (CESA-2012:1181)	Vulnerability - level 4	Vuln
120573	CentOS Security Update for TeTeX (CESA-2012:1201)	Vulnerability - level 4	Vuln
120578	CentOS Security Update for Firefox (CESA-2012:1210)	Vulnerability - level 4	Vuln
120579	CentOS Security Update for Thunderbird (CESA-2012:1211)	Vulnerability - level 4	Vuln
120617	CentOS Security Update for freeradius2 (CESA-2012:1327)	Vulnerability - level 3	Vuln
120618	CentOS Security Update for FreeRADIUS (CESA-2012:1326)	Vulnerability - level 3	Vuln
120619	CentOS Security Update for Kernel (CESA-2012:1323)	Vulnerability - level 4	Vuln
120630	CentOS Security Update for java-1.6.0-openjdk (CESA-2012:1221)	Vulnerability - level 3	Vuln
120631	CentOS Security Update for java-1.7.0-openjdk (CESA-2012:1223)	Vulnerability - level 4	Vuln
120635	CentOS Security Update for libexif (CESA-2012:1255)	Vulnerability - level 3	Vuln
120641	CentOS Security Update for libxslt (CESA-2012:1265)	Vulnerability - level 3	Vuln
120684	Red Hat Update for libproxy (RHSA-2012:1461)	Vulnerability - level 3	Vuln
120686	Red Hat Update for java-1.6.0-ibm (RHSA-2012:1466)	Vulnerability - level 5	Vuln
120688	Solaris "libtiff" Denial of Service Vulnerability	Vulnerability - level 3	Vuln
120728	Solaris Multiple Vulnerabilities in Firefox	Vulnerability - level 4	Vuln
120757	CentOS Security Update for libproxy (CESA-2012:1461)	Vulnerability - level 5	Vuln
120764	CentOS Security Update for libtiff (CESA-2012:1590)	Vulnerability - level 3	Vuln
120769	Red Hat Update for libtiff (RHSA-2012:1590)	Vulnerability - level 3	Vuln
120774	Siemens Automation License Manager Denial of Service Vulnerability (SSA-783261)	Vulnerability - level 3	Vuln
120779	CA XCOM Data Transport Remote Arbitrary Command Execution Vulnerability	Vulnerability - level 5	Vuln
120858	Ecava IntegraXor ActiveX Buffer Overflow	Vulnerability - level 5	Vuln
120879	Oracle Java SE Critical Patch Update - February 2013 Special Update	Vulnerability - level 4	Vuln
120886	Red Hat Update for java-1.6.0-openjdk (RHSA-2013:0273)	Vulnerability - level 5	Vuln
120887	Red Hat Update for java-1.6.0-openjdk (RHSA-2013:0274)	Vulnerability - level 4	Vuln
120888	Red Hat Update for java-1.7.0-openjdk (RHSA-2013:0275)	Vulnerability - level 4	Vuln
120889	Red Hat Update for java-1.6.0-sun (RHSA-2013:0531)	Vulnerability - level 5	Vuln
120890	Red Hat Update for java-1.7.0-oracle (RHSA-2013:0532)	Vulnerability - level 5	Vuln
120908	Solaris 11 Support Repository Update (SRU) 12.4 Missing	Vulnerability - level 3	Vuln
120969	Red Hat Update for libxml2 (RHSA-2013:0581)	Vulnerability - level 3	Vuln
120985	CentOS Security Update for java-1.6.0-openjdk (CESA-2013:0273)	Vulnerability - level 4	Vuln
120986	CentOS Security Update for java-1.7.0-openjdk (CESA-2013:0275)	Vulnerability - level 4	Vuln
120987	CentOS Security Update for java-1.6.0-openjdk (CESA-2013:0274)	Vulnerability - level 4	Vuln
120990	Red Hat Update for OpenSSL (RHSA-2013:0587)	Vulnerability - level 3	Vuln
120993	Red Hat Update for nss-pam-ldapd (RHSA-2013:0590)	Vulnerability - level 4	Vuln
121005	Red Hat Update for Ruby (RHSA-2013:0611)	Vulnerability - level 3	Vuln
121006	Red Hat Update for Ruby (RHSA-2013:0612)	Vulnerability - level 3	Vuln
121009	Red Hat Update for xulrunner (RHSA-2013:0614)	Vulnerability - level 5	Vuln
121011	Red Hat Update for tomcat6 (RHSA-2013:0623)	Vulnerability - level 4	Vuln
121015	Red Hat Update for Thunderbird (RHSA-2013:0627)	Vulnerability - level 4	Vuln
121021	Solaris Multiple Vulnerabilities in Apache Tomcat	Vulnerability - level 3	Vuln
121022	Solaris Multiple Vulnerabilities in libxslt	Vulnerability - level 3	Vuln
121027	Red Hat Update for sssd (RHSA-2013:0663)	Vulnerability - level 3	Vuln
121035	Red Hat Update for Perl (RHSA-2013:0685)	Vulnerability - level 3	Vuln
121037	IBM AIX OpenSSL Multiple Vulnerabilities	Vulnerability - level 3	Vuln

121043	Red Hat Update for BIND (RHSA-2013:0689)	Vulnerability - level 4	Vuln
121051	Adobe Flash Player and AIR Multiple Vulnerabilities (APSB13-11)	Vulnerability - level 4	Vuln
121053	Red Hat Update for KVM (RHSA-2013:0727)	Vulnerability - level 4	Vuln
121054	Red Hat Update for flash-plugin (RHSA-2013:0730)	Vulnerability - level 5	Vuln
121061	Oracle Java SE Critical Patch Update - April 2013	Vulnerability - level 5	Vuln
121066	Java for OS X 2013-003 and Mac OS X v10.6 Update 15 (APPLE-SA-2013-04-16-2)	Vulnerability - level 5	Vuln
121075	CentOS Security Update for KVM (CESA-2013:0727)	Vulnerability - level 3	Vuln
121076	CentOS Security Update for Subversion (CESA-2013:0737)	Vulnerability - level 3	Vuln
121080	CentOS Security Update for libxml2 (CESA-2013:0581)	Vulnerability - level 3	Vuln
121083	CentOS Security Update for OpenSSL (CESA-2013:0587)	Vulnerability - level 3	Vuln
121089	CentOS Security Update for XULRunner (CESA-2013:0614)	Vulnerability - level 5	Vuln
121116	CentOS Security Update for nss-pam-ldapd (CESA-2013:0590)	Vulnerability - level 3	Vuln
121118	CentOS Security Update for tomcat6 (CESA-2013:0623)	Vulnerability - level 3	Vuln
121119	CentOS Security Update for Thunderbird (CESA-2013:0627)	Vulnerability - level 5	Vuln
121121	CentOS Security Update for tomcat5 (CESA-2013:0640)	Vulnerability - level 3	Vuln
121124	CentOS Security Update for SSSD (CESA-2013:0663)	Vulnerability - level 2	Vuln
121127	CentOS Security Update for Perl (CESA-2013:0685)	Vulnerability - level 4	Vuln
121131	Red Hat Update for Subversion (RHSA-2013:0737)	Vulnerability - level 3	Vuln
121136	Red Hat Update for java-1.7.0-openjdk (RHSA-2013:0751)	Vulnerability - level 5	Vuln
121137	Red Hat Update for java-1.7.0-openjdk (RHSA-2013:0752)	Vulnerability - level 4	Vuln
121141	Red Hat Update for java-1.7.0-oracle (RHSA-2013:0757)	Vulnerability - level 5	Vuln
121142	Red Hat Update for java-1.6.0-sun (RHSA-2013:0758)	Vulnerability - level 5	Vuln
121143	Solaris 11.1 Support Repository Update (SRU) 2.5 Missing	Vulnerability - level 4	Vuln
121144	Solaris 11.1 Support Repository Update (SRU) 3.4 Missing	Vulnerability - level 3	Vuln
121147	Solaris 11.1 Support Repository Update (SRU) 4.5 Missing	Vulnerability - level 2	Vuln
121154	Red Hat Update for Kernel (RHSA-2013:0744)	Vulnerability - level 4	Vuln
121155	Red Hat Update for Java-1.6.0-openjdk (RHSA-2013:0770)	Vulnerability - level 4	Vuln
121162	Solaris Apache Ant Algorithmic Complexity Vulnerability	Vulnerability - level 3	Vuln
121163	Solaris Samba Web Administration Tool (SWAT) Multiple Vulnerabilities	Vulnerability - level 3	Vuln
121165	IBM Notes Arbitrary Java and Javascript Code Execution Vulnerability	Vulnerability - level 4	Vuln
121172	Red Hat Update for httpd (RHSA-2013:0815)	Vulnerability - level 3	Vuln
121181	Red Hat Update for java-1.7.0-ibm (RHSA-2013:0822)	Vulnerability - level 5	Vuln
121182	Red Hat Update for java-1.6.0-ibm (RHSA-2013:0823)	Vulnerability - level 5	Vuln
121188	Red Hat Update for libvirt (RHSA-2013:0831)	Vulnerability - level 3	Vuln
121192	Solaris 11.1 Support Repository Update (SRU) 7.5 Missing	Vulnerability - level 3	Vuln
121198	Red Hat Update for java-1.5.0-ibm (RHSA-2013:0855)	Vulnerability - level 4	Vuln
121200	IBM Java SDK Multiple Vulnerabilities - Oracle April 2013 CPU	Vulnerability - level 5	Vuln
121204	Wireshark Multiple Denial of Service Vulnerabilities (wnpa-sec-2013-23 - wnpa-sec-2013-31)	Vulnerability - level 3	Vuln
121206	Novell GroupWise Internet Agent Multiple Vulnerabilities	Vulnerability - level 3	Vuln
121219	Schneider Electric IGSS Data Server Remote Denial of Service Vulnerability	Vulnerability - level 3	Vuln
121226	Apple Mountain Lion v10.8.4 and Security Update 2013-002 Not Installed (APPLE-SA-2013-06-04-1)	Vulnerability - level 4	Vuln
121228	CentOS Security Update for java-1.7.0-openjdk (CESA-2013:0752)	Vulnerability - level 5	Vuln
121231	CentOS Security Update for Kernel (CESA-2013:0744)	Vulnerability - level 4	Vuln
121233	CentOS Security Update for java-1.6.0-openjdk (CESA-2013:0770)	Vulnerability - level 5	Vuln
121235	CentOS Security Update for java-1.7.0-openjdk (CESA-2013:0751)	Vulnerability - level 5	Vuln
121239	CentOS Security Update for httpd (CESA-2013:0815)	Vulnerability - level 2	Vuln
121245	CentOS Security Update for HAProxy (CESA-2013:0868)	Vulnerability - level 3	Vuln
121250	CentOS Security Update for libvirt (CESA-2013:0831)	Vulnerability - level 3	Vuln
121264	Red Hat Update for krb5 (RHSA-2013:0942)	Vulnerability - level 3	Vuln
121265	Solaris Lucky Thirteen Vulnerability in Solaris OpenSSL	Vulnerability - level 3	Vuln
121267	Solaris 10 Multiple Vulnerabilities in Apache HTTP server	Vulnerability - level 3	Vuln
121269	Solaris "libxml2" Denial of Service Vulnerability	Vulnerability - level 3	Vuln
121271	IBM Data Studio Multiple Vulnerabilities	Vulnerability - level 3	Vuln

121288	Red Hat Update for tomcat6 (RHSA-2013:0964)	Vulnerability - level 3	Vuln
121328	Linux Kernel libceph Authorization Client Remote Denial of Service Vulnerability	Potential Vulnerability - level 4	Practice
121339	Solaris Multiple Vulnerabilities in libexif	Vulnerability - level 3	Vuln
121343	Solaris 8 and 9 Multiple Vulnerabilities in Apache HTTP Server	Vulnerability - level 3	Vuln
121351	Red Hat Update for Ruby (RHSA-2013:1090)	Vulnerability - level 3	Vuln
121354	Autodesk Multiple Products DWG File Processing Arbitrary Code Execution Vulnerability	Vulnerability - level 3	Vuln
121368	OpenOffice.org Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
121372	Multiple PuTTY Products (PuTTY, WinSCP, FileZilla) Security Vulnerabilities	Vulnerability - level 4	Vuln
121389	Puppet Enterprise Multiple Vulnerabilities	Vulnerability - level 3	Vuln
121413	CentOS Security Update for tomcat6 (CESA-2013:0964)	Vulnerability - level 3	Vuln
121422	CentOS Security Update for Ruby (CESA-2013:1090)	Vulnerability - level 3	Vuln
121437	Red Hat Update for GDM (RHSA-2013:1213)	Vulnerability - level 4	Vuln
121441	ProSoft Technology RadioLinx ControlScape Weak PRNG Vulnerability	Vulnerability - level 4	Vuln
121449	Apache Subversion Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
121453	Solaris 11.1 Support Repository Update (SRU) 10.5.0 Missing	Vulnerability - level 4	Vuln
121456	Apple Mountain Lion v10.8.5 and Security Update 2013-004 Not Installed (APPLE-SA-2013-09-12-1)	Vulnerability - level 4	Vuln
121468	Apache Subversion "mod_dav_svn" Multiple Denial of Service Vulnerabilities	Vulnerability - level 3	Vuln
121469	Apache Subversion Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
121474	Solaris Denial of Service Vulnerability in Kerberos	Vulnerability - level 3	Vuln
121476	Solaris 11.1 Support Repository Update (SRU) 11.4.0 Missing	Vulnerability - level 4	Vuln
121494	Red Hat Update for samba3x (RHSA-2013:1310)	Vulnerability - level 3	Vuln
121495	Red Hat Update for php53 (RHSA-2013:1307)	Vulnerability - level 3	Vuln
121523	Red Hat Update for RubyGems (RHSA-2013:1441)	Vulnerability - level 3	Vuln
121526	Solaris Multiple Vulnerabilities in Apache HTTP Server	Vulnerability - level 3	Vuln
121528	Solaris Configuration Vulnerability in Perl	Vulnerability - level 3	Vuln
121547	Red Hat Update for gnupg (RHSA-2013:1458)	Vulnerability - level 3	Vuln
121549	Red Hat Update for gnupg2 (RHSA-2013:1459)	Vulnerability - level 3	Vuln
121561	Red Hat Update for postgresql and postgresql84 (RHSA-2013:1475)	Vulnerability - level 3	Vuln
121583	Google Chrome Prior to 31.0.1650.48 Multiple Vulnerabilities	Vulnerability - level 3	Vuln
121591	Mozilla Firefox / SeaMonkey NSS Multiple Vulnerabilities (MFSA-2013-103)	Vulnerability - level 4	Vuln
121599	Red Hat Update for Samba (RHSA-2013:1542)	Vulnerability - level 3	Vuln
121601	Red Hat Update for PHP (RHSA-2013:1615)	Vulnerability - level 3	Vuln
121602	Red Hat Update for 389-ds-base (RHSA-2013:1752)	Vulnerability - level 2	Vuln
121605	Red Hat Update for Kernel (RHSA-2013:1645)	Vulnerability - level 4	Vuln
121607	Red Hat Update for xorg-x11-server (RHSA-2013:1620)	Vulnerability - level 2	Vuln
121617	Red Hat Update for mod_nss (RHSA-2013:1779)	Vulnerability - level 3	Vuln
121626	Red Hat Update for libjpeg (RHSA-2013:1804)	Vulnerability - level 3	Vuln
121630	Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2013-104 through MFSA 2013-117)	Vulnerability - level 4	Vuln
121635	Red Hat Update for libjpeg-turbo (RHSA-2013:1803)	Vulnerability - level 3	Vuln
121636	Red Hat Update for PHP (RHSA-2013:1814)	Vulnerability - level 5	Vuln
121644	CentOS Security Update for gdm and initscripts (CESA-2013:1213)	Vulnerability - level 4	Vuln
121657	CentOS Security Update for rubygems (CESA-2013:1441)	Vulnerability - level 3	Vuln
121664	CentOS Security Update for gnupg2 (CESA-2013:1459)	Vulnerability - level 3	Vuln
121665	CentOS Security Update for gnupg (CESA-2013:1458)	Vulnerability - level 3	Vuln
121667	CentOS Security Update for postgresql (CESA-2013:1475)	Vulnerability - level 3	Vuln
121689	Avant Browser Rendering Engines Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
121690	GnuPG RSA Key Information Disclosure	Vulnerability - level 2	Vuln
121703	Red Hat Update for OpenSSL (RHSA-2014:0015)	Vulnerability - level 3	Vuln
121704	Red Hat Update for gnupg2 (RHSA-2014:0016)	Vulnerability - level 3	Vuln

121709	Ecava Sdn Bhd IntegraXor Project Directory Information Disclosure Vulnerability	Vulnerability - level 3	Vuln
121720	WellinTech KingSCADA, KingAlarm Event, and KingGraphic Multiple Vulnerabilities	Vulnerability - level 4	Vuln
121724	CentOS Security Update for mod_nss (CESA-2013:1779)	Vulnerability - level 3	Vuln
121731	CentOS Security Update for libjpeg (CESA-2013:1804)	Vulnerability - level 3	Vuln
121732	CentOS Security Update for libjpeg-turbo (CESA-2013:1803)	Vulnerability - level 3	Vuln
121735	CentOS Security Update for PHP (CESA-2013:1814)	Vulnerability - level 5	Vuln
121756	Apple iTunes Prior to 11.1.4 Multiple Vulnerabilities (HT6001)	Vulnerability - level 4	Vuln
121759	Solaris Denial of Service Vulnerability in libxslt	Vulnerability - level 3	Vuln
121767	3S CODESYS Runtime Toolkit Denial of Service Vulnerability	Vulnerability - level 3	Vuln
121768	MariaDB Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
121773	Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2014-01 through MFSA 2014-13)	Vulnerability - level 4	Vuln
121780	CentOS Security Update for gnupg (CESA-2014:0016)	Vulnerability - level 3	Vuln
121781	CentOS Security Update for OpenSSL (CESA-2014:0015)	Vulnerability - level 4	Vuln
121804	Red Hat Update for MySQL (RHSA-2014:0164)	Vulnerability - level 3	Vuln
121810	Red Hat Update for mysql55-mysql (RHSA-2014:0186)	Vulnerability - level 3	Vuln
121811	Red Hat Update for Openswan (RHSA-2014:0185)	Vulnerability - level 3	Vuln
121815	Apple Mac OS X v10.9.2 and Security Update 2014-001 Not Installed (APPLE-SA-2014-02-25-1)	Vulnerability - level 4	Vuln
121821	Red Hat Update for libtiff (RHSA-2014:0222)	Vulnerability - level 4	Vuln
121822	Red Hat Update for libtiff (RHSA-2014:0223)	Vulnerability - level 4	Vuln
121827	Red Hat Update for GnuTLS (RHSA-2014:0246)	Vulnerability - level 3	Vuln
121828	Red Hat Update for GnuTLS (RHSA-2014:0247)	Vulnerability - level 3	Vuln
121830	Red Hat Update for Subversion (RHSA-2014:0255)	Vulnerability - level 3	Vuln
121836	Solaris 11.1 Support Repository Update (SRU) 16.5.0 Missing	Vulnerability - level 4	Vuln
121842	Red Hat Update for Kernel (RHSA-2014:0285)	Vulnerability - level 4	Vuln
121852	Red Hat Update for Samba (RHSA-2014:0305)	Vulnerability - level 3	Vuln
121863	Red Hat Update for Kernel (RHSA-2014:0328)	Vulnerability - level 4	Vuln
121866	Adobe Flash Player Multiple Vulnerabilities (APSB14-09)	Vulnerability - level 4	Vuln
121867	Adobe Reader and Acrobat Multiple Vulnerabilities (APSB14-15)	Vulnerability - level 4	Vuln
121868	Solaris 11.1 Support Repository Update (SRU) 17.5.0 Missing	Vulnerability - level 3	Vuln
121874	Solaris Multiple vulnerabilities in Tomcat	Vulnerability - level 3	Vuln
121881	IBM AIX OpenSSL Denial of Service Vulnerability	Vulnerability - level 3	Vuln
121906	Fedora Security Update for gnutls (FEDORA-2014-3413)	Vulnerability - level 3	Vuln
121908	Fedora Security Update for libssh (FEDORA-2014-3485)	Vulnerability - level 3	Vuln
121916	Fedora Security Update for rubygem-actionpack (FEDORA-2014-3232)	Vulnerability - level 3	Vuln
121932	Fedora Security Update for mingw-gnutls (FEDORA-2014-3454)	Vulnerability - level 3	Vuln
121957	Fedora Security Update for Curl (FEDORA-2014-4436, FEDORA-2014-4449)	Vulnerability - level 3	Vuln
121962	CentOS Security Update for mysql (CESA-2014:0164)	Vulnerability - level 3	Vuln
121965	CentOS Security Update for openswan (CESA-2014:0185)	Vulnerability - level 3	Vuln
121966	CentOS Security Update for mysql55-mysql (CESA-2014:0186)	Vulnerability - level 3	Vuln
121967	CentOS Security Update for mysql55-mysql (CESA-2014:0173)	Vulnerability - level 3	Vuln
121970	CentOS Security Update for mariadb55-mariadb (CESA-2014:0189)	Vulnerability - level 3	Vuln
121971	CentOS Security Update for libtiff (CESA-2014:0223)	Vulnerability - level 3	Vuln
121972	CentOS Security Update for libtiff (CESA-2014:0222)	Vulnerability - level 3	Vuln
121976	CentOS Security Update for gnutls (CESA-2014:0247)	Vulnerability - level 4	Vuln
121978	CentOS Security Update for gnutls (CESA-2014:0246)	Vulnerability - level 4	Vuln
121979	CentOS Security Update for subversion (CESA-2014:0255)	Vulnerability - level 3	Vuln
121981	CentOS Security Update for kernel (CESA-2014:0285)	Vulnerability - level 4	Vuln
121984	CentOS Security Update for samba (CESA-2014:0305)	Vulnerability - level 3	Vuln
121986	CentOS Security Update for ruby193-rubygem-actionpack (CESA-2014:0306)	Vulnerability - level 3	Vuln
121993	CentOS Security Update for Kernel (CESA-2014:0328)	Vulnerability - level 4	Vuln
122001	Advantech WebAccess Multiple Vulnerabilities	Vulnerability - level 4	Vuln
122004	Red Hat Update for flash-plugin (RHSA-2014:0380)	Vulnerability - level 5	Vuln

122006	Solaris 11.1 Support Repository Update (SRU) 18.5.0 Missing	Vulnerability - level 3	Vuln
122007	Oracle Java SE Critical Patch Update - April 2014	Vulnerability - level 4	Vuln
122022	Red Hat Update for java-1.7.0-oracle (RHSA-2014:0413)	Vulnerability - level 5	Vuln
122023	Red Hat Update for java-1.7.0-oracle (RHSA-2014:0412)	Vulnerability - level 5	Vuln
122024	Red Hat Update for java-1.6.0-sun (RHSA-2014:0414)	Vulnerability - level 4	Vuln
122027	Progea Movicon SCADA Information Disclosure Vulnerability	Vulnerability - level 3	Vuln
122032	Red Hat Update for tomcat6 (RHSA-2014:0429)	Vulnerability - level 3	Vuln
122043	CentOS Security Update for tomcat6 (CESA-2014:0429)	Vulnerability - level 3	Vuln
122046	RAC Server IOCTL Handling Denial of Service Vulnerability	Vulnerability - level 3	Vuln
122063	Ecava IntegraXor Account Information Disclosure Vulnerability	Vulnerability - level 3	Vuln
122067	IBM Java SDK Multiple Vulnerabilities - Oracle April 2014 CPU	Vulnerability - level 4	Vuln
122069	Red Hat Update for Kernel (RHSA-2014:0475)	Vulnerability - level 4	Vuln
122074	Solaris Buffer Overflow Vulnerability in Texinfo	Vulnerability - level 3	Vuln
122078	Red Hat Update for java-1.7.0-ibm (RHSA-2014:0486)	Vulnerability - level 5	Vuln
122082	Red Hat Update for java-1.6.0-ibm (RHSA-2014:0508)	Vulnerability - level 5	Vuln
122083	Red Hat Update for java-1.5.0-ibm (RHSA-2014:0509)	Vulnerability - level 4	Vuln
122090	Solaris 11.1 Support Repository Update (SRU) 19.6.0 Missing	Vulnerability - level 4	Vuln
122092	TIBCO Rendezvous Prior To 8.4.2 Multiple Vulnerabilities	Vulnerability - level 4	Vuln
122095	Red Hat Update for curl (RHSA-2014:0561)	Vulnerability - level 3	Vuln
122103	CentOS Security Update for kernel (CESA-2014:0475)	Vulnerability - level 4	Vuln
122110	CentOS Security Update for curl (CESA-2014:0561)	Vulnerability - level 3	Vuln
122117	Red Hat Update for openssl (RHSA-2014:0625)	Vulnerability - level 4	Vuln
122120	OpenSSL Multiple Remote Security Vulnerabilities for Windows	Vulnerability - level 4	Vuln
122129	IBM AIX OpenSSL Race Condition Vulnerability	Vulnerability - level 3	Vuln
122130	IBM AIX OpenSSL Multiple Vulnerabilities	Vulnerability - level 3	Vuln
122136	Red Hat Update for Kernel (RHSA-2014:0771)	Vulnerability - level 4	Vuln
122141	CentOS Security Update for openssl (CESA-2014:0625)	Vulnerability - level 4	Vuln
122149	CentOS Security Update for Kernel (CESA-2014:0771)	Vulnerability - level 4	Vuln
122157	Fedora Security Update for openssl (FEDORA-2014-7102)	Vulnerability - level 3	Vuln
122160	Fedora Security Update for mingw-curl (FEDORA-2014-6921)	Vulnerability - level 3	Vuln
12217	Apache mod_auth_radius Malformed RADIUS Server Reply Integer Overflow Vulnerability	Potential Vulnerability - level 3	
12217	PHP cURL and GD Multiple Safe_Mode and Open_Basedir Restriction Bypass Vulnerabilities	Potential Vulnerability - level 3	Practice
122175	Fedora Security Update for mingw-libjpeg-turbo (FEDORA-2014-6859)	Vulnerability - level 3	Vuln
122178	Fedora Security Update for mingw-libpng (FEDORA-2014-6892)	Vulnerability - level 3	Vuln
12218	MPG123 Layer 2 Frame Header Heap Overflow Vulnerability	Potential Vulnerability - level 3	
12218	PHP Apache 2 Virtual() Safe_Mode and Open_Basedir Restriction Bypass Vulnerability	Potential Vulnerability - level 3	Practice
122208	Solaris 11.1 Support Repository Update (SRU) 20.5.0 Missing	Vulnerability - level 3	Vuln
122220	Cisco AnyConnect VPN Client OpenSSL Multiple Vulnerabilities	Vulnerability - level 3	Vuln
122324	Red Hat Update for tomcat6 (RHSA-2014:0865)	Vulnerability - level 3	Vuln
122332	Solaris 11.1 Support Repository Update (SRU) 21.4.1 Missing	Vulnerability - level 3	Vuln
122370	CentOS Security Update for tomcat6 (CESA-2014:0865)	Vulnerability - level 3	Vuln
122464	Fedora Security Update for zarafa (FEDORA-2014-7889)	Vulnerability - level 3	Vuln
122481	Red Hat Update for tomcat6 (RHSA-2014:1038)	Vulnerability - level 2	Vuln
12249	PHP Multiple Vulnerabilities May 2008	Vulnerability - level 3	Practice
12249	SGallery Module For PHPNuke SQL Injection Vulnerability	Vulnerability - level 3	
122490	Red Hat Update for openssl (RHSA-2014:1053)	Vulnerability - level 3	Vuln
122514	CentOS Security Update for tomcat (CESA-2014:1034)	Vulnerability - level 2	Vuln
122515	CentOS Security Update for tomcat6 (CESA-2014:1038)	Vulnerability - level 2	Vuln
122516	CentOS Security Update for openssl (CESA-2014:1053)	Vulnerability - level 3	Vuln
122517	CentOS Security Update for openssl (CESA-2014:1052)	Vulnerability - level 3	Vuln
122520	OpenOffice.org Information Disclosure and Command Execution Vulnerability	Vulnerability - level 3	Vuln
122529	Fedora Security Update for bugzilla (FEDORA-2014-8919)	Vulnerability - level 3	Vuln
122543	Fedora Security Update for trafficserver (FEDORA-2014-8790)	Vulnerability - level 3	Vuln

122546	Fedora Security Update for openssl (FEDORA-2014-9308)	Vulnerability - level 3	Vuln
122577	WinSCP OpenSSL Multiple Vulnerabilities	Vulnerability - level 3	Vuln
122591	Advantech WebAccess Multiple Vulnerabilities	Vulnerability - level 4	Vuln
122599	Fedora Security Update for jakarta-commons-httpclient (FEDORA-2014-9581)	Vulnerability - level 3	Vuln
12260	Apache HTTP Server Multiple Cross-Site Scripting Vulnerabilities	Vulnerability - level 4	Practice
12260	Sun Solaris Management Console User Interface Insecure Account Creation Vulnerability	Vulnerability - level 4	
122624	Fedora Security Update for httpcomponents-client (FEDORA-2014-9617)	Vulnerability - level 3	Vuln
122637	IBM AIX OpenSSL Multiple Vulnerabilities	Vulnerability - level 3	Vuln
122642	CentOS Security Update for httpcomponents-client (CESA-2014:1146)	Vulnerability - level 4	Vuln
122648	CentOS Security Update for jakarta-commons-httpclient (CESA-2014:1166)	Vulnerability - level 4	Vuln
122657	Solaris 11.2 Support Repository Update (SRU) 2.5.0 Missing	Vulnerability - level 4	Vuln
122660	Solaris GnuTLS Cryptographic Issues Vulnerability	Vulnerability - level 3	Vuln
122662	Solaris Firefox ESR Multiple Vulnerabilities	Vulnerability - level 4	Vuln
122664	Ecava Integraxor SCADA Server Multiple Vulnerabilities	Vulnerability - level 3	Vuln
122671	Fedora Security Update for smack (FEDORA-2014-9694)	Vulnerability - level 3	Vuln
122687	Fedora Security Update for libreoffice (FEDORA-2014-1073)	Vulnerability - level 3	Vuln
122690	Apple Mac OS X v10.9.5 and Security Update 2014-004 Not Installed (HT6443)	Vulnerability - level 4	Vuln
122789	Red Hat Update for openssl (RHSA-2014:1052)	Vulnerability - level 3	Vuln
122798	Solaris WAN Boot Multiple Vulnerabilities	Vulnerability - level 3	Vuln
122802	Solaris OpenSSL Information Disclosure Vulnerability	Vulnerability - level 3	Vuln
122824	LibreOffice Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
122873	MatrikonOPC Server for DNP3 Denial of Service Vulnerability	Vulnerability - level 3	Vuln
122886	Debian Security Update for gnutls26 (DSA 2869-1)	Vulnerability - level 3	Vuln
122896	Debian Security Update for libssh (DSA 2879-1)	Vulnerability - level 3	Vuln
122934	Fedora Security Update for bugzilla (FEDORA-2014-1259)	Vulnerability - level 3	Vuln
122962	Fedora Security Update for aircrack-ng (FEDORA-2014-1428)	Vulnerability - level 3	Vuln
122964	Fedora Security Update for curl (FEDORA-2014-1433)	Vulnerability - level 3	Vuln
122965	Fedora Security Update for curl (FEDORA-2014-1435)	Vulnerability - level 3	Vuln
122975	Fedora Security Update for aircrack-ng (FEDORA-2014-1423)	Vulnerability - level 3	Vuln
123043	Red Hat Update for jasper (RHSA-2014:2021)	Vulnerability - level 3	Vuln
123062	CentOS Security Update for jasper (CESA-2014:2021)	Vulnerability - level 4	Vuln
123071	Cogent DataHub Multiple Vulnerabilities	Vulnerability - level 3	Vuln
123072	Schneider Electric ProClima Multiple Buffer Overflow Vulnerabilities	Vulnerability - level 3	Vuln
123075	Solaris 11.2 Support Repository Update (SRU) 5.5.0 Missing	Vulnerability - level 4	Vuln
123082	EMC Connectrix Manager Converged Network Edition Information Disclosure Vulnerability	Vulnerability - level 3	Vuln
123093	Fedora Security Update for mingw-openssl (FEDORA-2014-17576)	Vulnerability - level 4	Vuln
123094	Fedora Security Update for mingw-dbus (FEDORA-2014-17595)	Vulnerability - level 3	Vuln
123095	Fedora Security Update for mingw-dbus (FEDORA-2014-17570)	Vulnerability - level 3	Vuln
123097	Fedora Security Update for mingw-curl (FEDORA-2014-17596)	Vulnerability - level 4	Vuln
123101	Fedora Security Update for curl (FEDORA-2014-16690)	Vulnerability - level 4	Vuln
123105	Fedora Security Update for ettercap (FEDORA-2014-17090)	Vulnerability - level 3	Vuln
123109	Fedora Security Update for kernel (FEDORA-2014-17244)	Vulnerability - level 3	Vuln
123112	Fedora Security Update for subversion (FEDORA-2014-17118)	Vulnerability - level 3	Vuln
123115	Fedora Security Update for jasper (FEDORA-2014-16349)	Vulnerability - level 3	Vuln
123116	Fedora Security Update for jasper (FEDORA-2014-16465)	Vulnerability - level 3	Vuln
123119	Fedora Security Update for jasper (FEDORA-2014-16292)	Vulnerability - level 3	Vuln
123142	Mozilla Firefox / Thunderbird / SeaMonkey Multiple Vulnerabilities (MFSA 2015-01 to MFSA 2015-09)	Vulnerability - level 4	Vuln
123144	Fedora Security Update for curl (FEDORA-2015-0418)	Vulnerability - level 4	Vuln
123147	Fedora Security Update for kernel (FEDORA-2015-0517)	Vulnerability - level 3	Vuln
123149	Fedora Security Update for smack (FEDORA-2015-0046)	Vulnerability - level 3	Vuln

123150	Fedora Security Update for openssl (FEDORA-2015-0512)	Vulnerability - level 4	Vuln
123151	Fedora Security Update for kernel (FEDORA-2015-0515)	Vulnerability - level 3	Vuln
123155	Debian Security Update for openssl (DSA 3125-1)	Vulnerability - level 4	Vuln
123180	Fedora Security Update for openssl (FEDORA-2015-0601)	Vulnerability - level 4	Vuln
123184	Red Hat Update for openssl (RHSA-2015:0066)	Vulnerability - level 3	Vuln
123186	Fedora Security Update for xen (FEDORA-2015-0331)	Vulnerability - level 3	Vuln
123201	Debian Security Update for linux (DSA 3128-1)	Vulnerability - level 4	Vuln
123220	CentOS Security Update for openssl (CESA-2015:0066)	Vulnerability - level 3	Vuln
123235	Fedora Security Update for kernel (FEDORA-2015-0937)	Vulnerability - level 3	Vuln
123239	Fedora Security Update for docker-io (FEDORA-2015-1128)	Vulnerability - level 3	Vuln
123242	Fedora Security Update for python-django14 (FEDORA-2015-0804)	Vulnerability - level 4	Vuln
123267	IBM AIX OpenSSL Multiple Vulnerabilities	Vulnerability - level 3	Vuln
12327	Ghostscript Multiple Local Insecure Temporary File Creation Vulnerabilities	Vulnerability - level 2	
12327	Mozilla Bugzilla Information Disclosure Weaknesses Version Prior to 3.4.5 or 3.5.3	Vulnerability - level 2	Vuln
123278	Symantec Data Center Security: Server Advanced and Symantec Critical System Protection Multiple Vulnerabilities	Vulnerability - level 5	Vuln
123279	Red Hat Update for subversion (RHSA-2015:0166)	Vulnerability - level 3	Vuln
123294	CentOS Security Update for subversion (CESA-2015:0166)	Vulnerability - level 3	Vuln
123300	Fedora Security Update for mingw-jasper (FEDORA-2015-1068)	Vulnerability - level 4	Vuln
123308	Fedora Security Update for kernel (FEDORA-2015-1657)	Vulnerability - level 3	Vuln
123310	Fedora Security Update for kernel (FEDORA-2015-1672)	Vulnerability - level 3	Vuln
123315	Fedora Security Update for jasper (FEDORA-2015-1062)	Vulnerability - level 4	Vuln
123316	Fedora Security Update for jasper (FEDORA-2015-1159)	Vulnerability - level 4	Vuln
123321	Fedora Security Update for ntp (FEDORA-2015-1759)	Vulnerability - level 4	Vuln
123328	Fedora Security Update for bugzilla (FEDORA-2015-1713)	Vulnerability - level 3	Vuln
123329	Fedora Security Update for bugzilla (FEDORA-2015-1699)	Vulnerability - level 3	Vuln
123330	Fedora Security Update for community-mysql (FEDORA-2015-1162)	Vulnerability - level 3	Vuln
123331	Fedora Security Update for ntp (FEDORA-2015-1736)	Vulnerability - level 4	Vuln
123336	Fedora Security Update for dbus (FEDORA-2015-2007)	Vulnerability - level 3	Vuln
123348	Fedora Security Update for apache-poi (FEDORA-2015-2087)	Vulnerability - level 3	Vuln
123349	Fedora Security Update for tomcat (FEDORA-2015-2109)	Vulnerability - level 3	Vuln
123355	Solaris 11.2 Support Repository Update (SRU) 6.5.0 Missing	Vulnerability - level 3	Vuln
123373	Red Hat Update for libreoffice (RHSA-2015:0377)	Vulnerability - level 3	Vuln
123401	SCADA Engine BACnet OPC Server Multiple Vulnerabilities (ICSA-15-069-03)	Vulnerability - level 3	Vuln
123408	OpenSSL Multiple Vulnerabilities (OpenSSL Security Advisory 20150319)	Vulnerability - level 4	Practice
123410	OpenSSL Multiple Denial of Service and Memory Corruption Vulnerabilities	Vulnerability - level 3	Practice
123423	Fedora Security Update for libjpeg-turbo (FEDORA-2015-2580)	Vulnerability - level 3	Vuln
123425	Fedora Security Update for kernel (FEDORA-2015-3011)	Vulnerability - level 3	Vuln
123449	Fedora Security Update for kernel (FEDORA-2015-3594)	Vulnerability - level 4	Vuln
123450	Fedora Security Update for gnupg (FEDORA-2015-3253)	Vulnerability - level 3	Vuln
123452	Fedora Security Update for ImageMagick (FEDORA-2015-3605)	Vulnerability - level 3	Vuln
123460	Fedora Security Update for ettercap (FEDORA-2015-4009)	Vulnerability - level 3	Vuln
123467	Fedora Security Update for kernel (FEDORA-2015-4059)	Vulnerability - level 4	Vuln
123470	Fedora Security Update for xen (FEDORA-2015-3721)	Vulnerability - level 3	Vuln
123471	Fedora Security Update for openssl (FEDORA-2015-4320)	Vulnerability - level 3	Vuln
123477	Fedora Security Update for openssl (FEDORA-2015-4300)	Vulnerability - level 3	Vuln
123483	CentOS Security Update for openssl (CESA-2015:0715)	Vulnerability - level 3	Vuln
123485	Red Hat Update for openssl (RHSA-2015:0716)	Vulnerability - level 3	Vuln
123486	Red Hat Update for openssl (RHSA-2015:0715)	Vulnerability - level 3	Vuln
123494	Schneider Electric InduSoft Web Studio Multiple Information Disclosure Vulnerabilities	Vulnerability - level 3	Vuln
123502	Ecava Integraxor SCADA Server Untrusted Search Path Vulnerability	Vulnerability - level 3	Vuln

123503	Inductive Automation Ignition Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
123506	Oracle Solaris 10 Multiple Vulnerabilities (Third Party Bulletin - January 2015)	Vulnerability - level 4	Vuln
123508	Solaris 11.2 Support Repository Update (SRU) 8.5.0 Missing	Vulnerability - level 3	Vuln
123515	Apple Mac OS X v10.10.3 and Security Update 2015-004 Not Installed (APPLE-SA-2015-04-08-2)	Vulnerability - level 5	Vuln
123521	Red Hat Update for openssl (RHSA-2015:0800)	Vulnerability - level 3	Vuln
123523	Solaris 11.2 Support Repository Update (SRU) 9.5.0 Missing	Vulnerability - level 3	Vuln
123526	IBM AIX OpenSSL Multiple Denial of Service Vulnerabilities	Vulnerability - level 3	Vuln
123549	CentOS Security Update for openssl (CESA-2015:0716)	Vulnerability - level 3	Vuln
123555	CentOS Security Update for openssl (CESA-2015:0800)	Vulnerability - level 3	Vuln
123566	Oracle Solaris 10 Multiple Vulnerabilities (Third Party Bulletin - April 2015)	Vulnerability - level 4	Vuln
123567	IBM Java SDK Multiple Vulnerabilities (Oracle April 2015 CPU and IBM Security Update May 2015)	Vulnerability - level 4	Vuln
123581	OpenSSL Multiple Denial of Service Vulnerabilities (secadv_20150611)	Vulnerability - level 3	Practice
123582	Red Hat Update for wpa_supplicant (RHSA-2015:1090)	Vulnerability - level 3	Vuln
123584	Red Hat Update for openssl (RHSA-2015:1115)	Vulnerability - level 3	Vuln
123585	Red Hat Update for gnutls (RHSA-2014:0288)	Vulnerability - level 4	Vuln
123589	Solaris 11.2 Support Repository Update (SRU) 11.5.0 Missing	Vulnerability - level 4	Vuln
123605	Fedora Security Update for nss (FEDORA-2015-9161)	Vulnerability - level 3	Vuln
123606	Fedora Security Update for nss-softokn (FEDORA-2015-9161)	Vulnerability - level 3	Vuln
123607	Fedora Security Update for nss-util (FEDORA-2015-9161)	Vulnerability - level 3	Vuln
123639	Fedora Security Update for qpid-cpp (FEDORA-2015-9503)	Vulnerability - level 3	Vuln
123641	Fedora Security Update for openssl (FEDORA-2015-10108)	Vulnerability - level 4	Vuln
123660	Red Hat Update for nss (RHSA-2015:1185)	Vulnerability - level 3	Vuln
123665	CentOS Security Update for wpa_supplicant (CESA-2015:1090)	Vulnerability - level 4	Vuln
123666	CentOS Security Update for openssl (CESA-2015:1115)	Vulnerability - level 3	Vuln
123672	CentOS Security Update for nss (CESA-2015:1185)	Vulnerability - level 3	Vuln
123679	IBM AIX NTPv4 Multiple Vulnerabilities	Vulnerability - level 3	Vuln
123680	Apple Mac OS X v10.10.4 and Security Update 2015-005 Not Installed (APPLE-SA-2015-06-30-2)	Vulnerability - level 4	Vuln
123682	Red Hat Update for openssl (RHSA-2015:1197)	Vulnerability - level 3	Vuln
123689	Red Hat Update for kernel (RHSA-2014:0634)	Vulnerability - level 4	Vuln
123695	Red Hat Update for kernel (RHSA-2014:0284)	Vulnerability - level 4	Vuln
123700	CentOS Security Update for openssl (CESA-2015:1197)	Vulnerability - level 3	Vuln
123706	IBM Tivoli Directory Server Server Multiple Vulnerabilities (swg21960659)	Vulnerability - level 4	Vuln
123714	Oracle Java SE Critical Patch Update - July 2015	Vulnerability - level 4	Vuln
123715	Solaris 11.2 Support Repository Update (SRU) 12.5.0 Missing	Vulnerability - level 3	Vuln
123718	Oracle Solaris 10 Multiple Vulnerabilities (Third Party Bulletin - July 2015)	Vulnerability - level 3	Vuln
123723	Oracle JRockit Multiple Vulnerabilities (CPUJUL2015)	Vulnerability - level 4	Vuln
123724	IBM AIX OpenSSL Multiple Vulnerabilities	Vulnerability - level 3	Vuln
123725	Red Hat Update for java-1.7.0-openjdk (RHSA-2015:1230)	Vulnerability - level 4	Vuln
123726	Red Hat Update for java-1.7.0-openjdk (RHSA-2015:1229)	Vulnerability - level 5	Vuln
123727	Red Hat Update for java-1.8.0-openjdk (RHSA-2015:1228)	Vulnerability - level 4	Vuln
123729	Red Hat Update for java-1.8.0-oracle (RHSA-2015:1241)	Vulnerability - level 5	Vuln
123730	Red Hat Update for java-1.7.0-oracle (RHSA-2015:1242)	Vulnerability - level 5	Vuln
123733	CentOS Security Update for java-1.7.0-openjdk (CESA-2015:1229)	Vulnerability - level 5	Vuln
123734	CentOS Security Update for java-1.8.0-openjdk (CESA-2015:1228)	Vulnerability - level 4	Vuln
123735	CentOS Security Update for java-1.7.0-openjdk (CESA-2015:1230)	Vulnerability - level 4	Vuln
123736	Red Hat Update for java-1.6.0-sun (RHSA-2015:1243)	Vulnerability - level 4	Vuln
123740	Google Chrome Prior to 44.0.2403.89 Multiple Vulnerabilities	Vulnerability - level 4	Vuln
123752	Red Hat Update for curl (RHSA-2015:1254)	Vulnerability - level 3	Vuln
123755	Red Hat Update for ntp (RHSA-2015:1459)	Vulnerability - level 3	Vuln
123761	IBM Java SDK Privilege Escalation Vulnerability (IBM Security Update June 2015)	Vulnerability - level 3	Vuln

123763	IBM Java SDK Multiple Vulnerabilities (Oracle July 14 2015 CPU)	Vulnerability - level 4	Vuln
123766	Red Hat Update for java-1.7.1-ibm (RHSA-2015:1485)	Vulnerability - level 5	Vuln
123767	Red Hat Update for java-1.6.0-ibm (RHSA-2015:1486)	Vulnerability - level 5	Vuln
123770	Red Hat Update for java-1.7.0-ibm (RHSA-2015:1488)	Vulnerability - level 5	Vuln
123772	Red Hat Update for chromium-browser (RHSA-2015:1499)	Vulnerability - level 4	Vuln
123787	Red Hat Update for java-1.6.0-openjdk (RHSA-2015:1526)	Vulnerability - level 4	Vuln
123789	Red Hat Update for java-1.5.0-ibm (RHSA-2015:1544)	Vulnerability - level 4	Vuln
12379	Juniper Networks JUNOS Unspecified Remote Denial Of Service Vulnerability	Potential Vulnerability - level 3	
12379	TaskFreak Cross-Site Scripting and SQL Injection Vulnerabilities	Potential Vulnerability - level 3	Practice
123806	Apple Mac OS X v10.10.5 and Security Update 2015-006 Not Installed (APPLE-SA-2015-08-13-2)	Vulnerability - level 4	Vuln
123813	Red Hat Update for subversion (RHSA-2015:1633)	Vulnerability - level 3	Vuln
123824	IBM AIX "Sendmail" Diffie-Hellman Ciphers Vulnerability	Vulnerability - level 3	Vuln
123825	Solaris 11.2 Support Repository Update (SRU) 13.6.0 Missing	Vulnerability - level 4	Vuln
123833	IBM AIX NTPv3 Vulnerability	Vulnerability - level 3	Vuln
123843	CentOS Security Update for java-1.6.0-openjdk (CESA-2015:1526)	Vulnerability - level 4	Vuln
123853	CentOS Security Update for subversion (CESA-2015:1633)	Vulnerability - level 3	Vuln
123866	Red Hat Update for jakarta-taglibs-standard (RHSA-2015:1695)	Vulnerability - level 4	Vuln
123870	FortiClient Antivirus Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
123888	Fedora Security Update for rubygems (FEDORA-2015-12574)	Vulnerability - level 3	Vuln
123920	Fedora Security Update for rubygems (FEDORA-2015-13157)	Vulnerability - level 3	Vuln
123932	Fedora Security Update for openssh (FEDORA-2015-13469)	Vulnerability - level 3	Vuln
123944	Red Hat Update for subversion (RHSA-2015:1742)	Vulnerability - level 3	Vuln
123946	IBM AIX OpenSSH Vulnerability	Vulnerability - level 3	Vuln
123950	CentOS Security Update for jakarta-taglibs-standard (CESA-2015:1695)	Vulnerability - level 4	Vuln
123958	CentOS Security Update for subversion (CESA-2015:1742)	Vulnerability - level 3	Vuln
123959	Red Hat Update for openssl security (RHSA-2016:0996)	Vulnerability - level 4	Vuln
123973	IBM WebSphere Application Server Prior to 6.1.0.47 Multiple Vulnerabilities (swg21647522)	Vulnerability - level 3	Practice
123974	IBM WebSphere Application Server Multiple Vulnerabilities (swg21644047)	Vulnerability - level 3	Practice
123983	Fedora Security Update for trafficserver (FEDORA-2015-10520)	Vulnerability - level 3	Vuln
123990	Fedora Security Update for openssh (FEDORA-2015-11067)	Vulnerability - level 3	Vuln
123993	Fedora Security Update for openssh (FEDORA-2015-11063)	Vulnerability - level 3	Vuln
124038	Fedora Security Update for subversion (FEDORA-2015-11795)	Vulnerability - level 3	Vuln
124090	Fedora Security Update for ntp (FEDORA-2015-14213)	Vulnerability - level 3	Vuln
124107	Fedora Security Update for freeimage (FEDORA-2015-16106)	Vulnerability - level 3	Vuln
124124	CentOS Security Update for curl (CESA-2015:1254)	Vulnerability - level 3	Vuln
124132	CentOS Security Update for ntp (CESA-2015:1459)	Vulnerability - level 3	Vuln
124142	Apple Safari 9.0 Not Installed (APPLE-SA-2015-09-30-2)	Vulnerability - level 4	Vuln
124155	IBM WebSphere Application Server Multiple Vulnerabilities (swg21676092, swg21669554)	Vulnerability - level 3	Practice
124156	IBM WebSphere Application Server Multiple Vulnerabilities (swg21651880)	Vulnerability - level 3	Practice
124157	IBM WebSphere Application Server Multiple Vulnerabilities (swg21681249, swg21676091, swg21676092)	Vulnerability - level 3	Practice
124160	CODESYS 3S Gateway Null Pointer Exception Vulnerability	Vulnerability - level 3	Vuln
124172	Apple Mac OS X v10.11.1 Not Installed (APPLE-SA-2015-10-21-4)	Vulnerability - level 4	Vuln
124180	IBM AIX "OpenSSH" Local Privilege Escalation Vulnerabilities	Vulnerability - level 3	Vuln
124182	Apple Mac OS X Security Update 2015-007 Not Installed (APPLE-SA-2015-10-21-4)	Vulnerability - level 4	Vuln
124183	Red Hat Update for ntp (RHSA-2015:1930)	Vulnerability - level 3	Vuln
124201	IBM AppScan Remote Code Execution Vulnerability	Vulnerability - level 3	Vuln
124202	IBM Security AppScan Enterprise Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
124221	CentOS Security Update for ntp (CESA-2015:1930)	Vulnerability - level 4	Vuln

124244	Red Hat Update for ntp (RHSA-2015:2231)	Vulnerability - level 3	Vuln
124253	Red Hat Update for openssh (RHSA-2015:2088)	Vulnerability - level 3	Vuln
124264	Red Hat Update for unbound (RHSA-2015:2455)	Vulnerability - level 3	Vuln
124268	Red Hat Update for curl (RHSA-2015:2159)	Vulnerability - level 3	Vuln
124279	Tibbo AggreGate Platform Multiple Vulnerabilities	Vulnerability - level 3	Vuln
124283	Red Hat Update for ntp (RHSA-2015:2520)	Vulnerability - level 3	Vuln
124332	Fedora Security Update for ntp (FEDORA-2015-77)	Vulnerability - level 3	Vuln
124382	OpenSSL Multiple Vulnerabilities (OpenSSL Security Advisory 20151203)	Vulnerability - level 3	Practice
124389	Apple Mac OS X v10.11.2 and Security Update 2015-008 Not Installed (APPLE-SA-2015-12-08-3)	Vulnerability - level 4	Vuln
124399	Red Hat Update for openssl (RHSA-2015:2616)	Vulnerability - level 3	Vuln
124400	Red Hat Update for openssl (RHSA-2015:2617)	Vulnerability - level 3	Vuln
124405	Schneider Electric ProClima Multiple Buffer Overflow Vulnerabilities	Vulnerability - level 3	Vuln
124409	IBM AIX RC4(Arcfour) Stream Cipher Vulnerability	Vulnerability - level 3	Vuln
124426	Unitronics VisiLogic OPLC IDE Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
124441	Fedora Security Update for openssl (FEDORA-2015-605)	Vulnerability - level 3	Vuln
124480	CentOS Security Update for curl (CESA-2015:2159)	Vulnerability - level 3	Vuln
124490	CentOS Security Update for ntp (CESA-2015:2231)	Vulnerability - level 3	Vuln
124493	CentOS Security Update for openssh (CESA-2015:2088)	Vulnerability - level 3	Vuln
124503	CentOS Security Update for unbound (CESA-2015:2455)	Vulnerability - level 2	Vuln
124512	CentOS Security Update for openssl (CESA-2015:2617)	Vulnerability - level 3	Vuln
124513	CentOS Security Update for openssl (CESA-2015:2616)	Vulnerability - level 3	Vuln
124561	Fedora Security Update for gajim (FEDORA-2016-838200213)	Vulnerability - level 3	Vuln
124563	Advantech WebAccess Multiple Security Vulnerabilities	Vulnerability - level 4	Vuln
124564	IBM AIX OpenSSL Multiple Vulnerabilities	Vulnerability - level 3	Vuln
124566	Solaris 11.3 Support Repository Update (SRU) 4.5.0 Missing	Vulnerability - level 3	Vuln
124568	Oracle Solaris 10 Multiple Vulnerabilities (Third Party Bulletin - January 2016)	Vulnerability - level 3	Vuln
124574	Fedora Security Update for openssh (FEDORA-2016-67)	Vulnerability - level 3	Vuln
124600	IBM AIX NTP Multiple Vulnerabilities	Vulnerability - level 3	Vuln
124628	FreeBSD Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
124630	F5 BIG-IP ASM Multiple OpenSSL Vulnerabilities (SOL86772626, SOL55540723)	Vulnerability - level 4	Vuln
124631	F5 BIG-IP ASM OpenSSL Information Disclosure Vulnerability (SOL12824341)	Vulnerability - level 3	Vuln
124634	Fedora Security Update for gsi-openssh (FEDORA-2016-4556904561)	Vulnerability - level 3	Vuln
124635	Fedora Security Update for openssl (FEDORA-2016-527018d2ff)	Vulnerability - level 4	Vuln
124640	Fedora Security Update for ntp (FEDORA-2016-8bb1932088)	Vulnerability - level 3	Vuln
124644	IBM AIX OpenSSH Multiple Vulnerabilities	Vulnerability - level 3	Vuln
124645	IBM AIX NTP Multiple Vulnerabilities	Vulnerability - level 3	Vuln
124648	Red Hat Update for openssl security (RHSA-2016:0722)	Vulnerability - level 4	Vuln
124653	Fedora Security Update for gsi-openssh (FEDORA-2016-2e89eba0c1)	Vulnerability - level 3	Vuln
124660	CentOS Security Update for ntp Security Update (CESA-2016:0063)	Vulnerability - level 4	Vuln
124684	F5 BIG-IP ASM OpenSSL a_type.c Denial-of-Service Vulnerability (SOL16317)	Vulnerability - level 3	Vuln
124685	F5 BIG-IP ASM OpenSSL Multiple Denial-of-Service Vulnerabilities (SOL16321, SOL16323)	Vulnerability - level 3	Vuln
124703	Fedora Security Update for gsi-openssh (FEDORA-2016-4509765b4b)	Vulnerability - level 3	Vuln
124748	Solaris 11.3 Support Repository Update (SRU) 5.6.0 Missing	Vulnerability - level 3	Vuln
124749	IBM AIX Network Time Protocol (NTPv4) Vulnerability	Vulnerability - level 3	Vuln
124754	Red Hat Update for openssl (RHSA-2016:0301)	Vulnerability - level 3	Vuln
124755	Red Hat Update for openssl (RHSA-2016:0302)	Vulnerability - level 3	Vuln
124756	Red Hat Update for openssl (RHSA-2016:0305)	Vulnerability - level 3	Vuln
124757	Red Hat Update for openssl (RHSA-2016:0306)	Vulnerability - level 3	Vuln

124760	IBM AIX OpenSSL Multiple Vulnerabilities	Vulnerability - level 3	Vuln
124766	OpenSSH "X SECURITY" Bypass Vulnerability	Vulnerability - level 3	Vuln
124770	Red Hat Update for openssl098e (RHSA-2016:0372)	Vulnerability - level 3	Vuln
124775	F5 BIG-IP ASM Multiple OpenSSL Denial-of-Service Vulnerabilities (SOL86772626, SOL55540723)	Vulnerability - level 3	Vuln
124776	F5 BIG-IP ASM OpenSSL Information Disclosure Vulnerability (SOL12824341)	Vulnerability - level 3	Vuln
124780	Red Hat Update for xerces-c (RHSA-2016:0430)	Vulnerability - level 3	Vuln
124839	Red Hat Update for openssh (RHSA-2016:0465)	Vulnerability - level 3	Vuln
124841	Solaris 11.3 Support Repository Update (SRU) 6.5.0 Missing	Vulnerability - level 3	Vuln
124842	Apple Mac OS X v10.11.4 and Security Update 2016-002 Not Installed (APPLE-SA-2016-03-21-5)	Vulnerability - level 4	Vuln
124859	CentOS Security Update for openssl (CESA-2016:0301)	Vulnerability - level 4	Vuln
124860	CentOS Security Update for openssl (CESA-2016:0302)	Vulnerability - level 4	Vuln
124870	Red Hat Update for JBoss Enterprise Application Platform 6.1.1 (RHSA-2013:1207,RHSA-2013:1208)	Vulnerability - level 3	Vuln
124871	IBM AIX OpenSSL Multiple Vulnerabilities	Vulnerability - level 4	Vuln
124878	Solaris 11.3 Support Repository Update (SRU) 7.6.0 Missing	Vulnerability - level 4	Vuln
124883	Oracle Solaris 10 Multiple Vulnerabilities (Third Party Bulletin - April 2016)	Vulnerability - level 4	Vuln
124909	CentOS Security Update for openssl098e (CESA-2016:0372)	Vulnerability - level 4	Vuln
124914	CentOS Security Update for xerces-c (CESA-2016:0430)	Vulnerability - level 4	Vuln
124922	CentOS Security Update for openssh (CESA-2016:0465)	Vulnerability - level 3	Vuln
124934	Ecava Integraxor Scada Server SQL Injection Remote Code Execution Vulnerability	Vulnerability - level 3	Vuln
124945	IBM AIX OpenSSH Remote Code Execution Vulnerability	Vulnerability - level 4	Vuln
124950	IBM AIX OpenSSL Denial of Service Vulnerability	Vulnerability - level 4	Vuln
124979	Fedora Security Update for qpid-cpp (FEDORA-2016-120b194a75)	Vulnerability - level 3	Vuln
12556	ELOG Web Logbook Multiple Remote Vulnerabilities	Potential Vulnerability - level 3	
12556	Mapserver for Windows Local File Include Vulnerability	Potential Vulnerability - level 3	Practice
12591	Mozilla Bugzilla Multiple Information Disclosure Vulnerabilities	Potential Vulnerability - level 3	Practice
12591	Tarantella Enterprise/Secure Global Desktop Remote Information Disclosure Vulnerability	Potential Vulnerability - level 3	
12625	MediaWiki Multiple Unspecified Remote Vulnerabilities	Potential Vulnerability - level 3	
12625	Mozilla Bugzilla Multiple Cross-Site Scripting and Information Disclosure Vulnerabilities	Potential Vulnerability - level 3	Practice
12629	IBM Hardware Management Console Guided Setup Wizard Unauthorized Access Vulnerability	Potential Vulnerability - level 3	
12629	Ruby on Rails Multiple Cross-Site Scripting Vulnerabilities	Potential Vulnerability - level 3	Practice
12655	Mozilla Firefox Scrollbar Remote Code Execution Vulnerability	Vulnerability - level 3	
12655	Ruby on Rails Multiple Vulnerabilities	Vulnerability - level 3	Vuln
12696	PHP Heap Based Buffer Overflow Vulnerability	Potential Vulnerability - level 3	Practice
12696	PHPNews Auth.PHP Remote File Include Vulnerability	Potential Vulnerability - level 3	
12699	phpMyAdmin Cross-Site Scripting Vulnerability (PMASA-2013-6)	Potential Vulnerability - level 3	Practice
12752	OutStart Participate Enterprise Multiple Access Validation Vulnerabilities	Potential Vulnerability - level 3	
12752	PHP Multiple Arbitrary File Access Vulnerabilities	Potential Vulnerability - level 3	Practice
12767	Moodle badges/external.php Cross-Site Scripting Vulnerability	Vulnerability - level 3	Vuln
12767	Perl Local Race Condition Privilege Escalation Vulnerability	Vulnerability - level 3	

12781	Multiple EMC Documentum Products Cross-Site Scripting Vulnerability (ESA-2013-070)	Potential Vulnerability - level 3	Practice
12781	MySQL AB MySQL Multiple Remote Vulnerabilities	Potential Vulnerability - level 3	
12823	ASPJar Guestbook Tell-a-Friend Cross-Site Scripting Vulnerability	Potential Vulnerability - level 3	
12823	EMC Documentum eRoom Multiple Unspecified Cross-Site Scripting Vulnerabilities (ESA-2013-073)	Potential Vulnerability - level 3	Practice
12825	EMC Documentum eRoom Arbitrary File Upload Vulnerability (ESA-2011-032)	Potential Vulnerability - level 3	Practice
12825	Multiple BSD Vendor Copyout Destination Address Verification Vulnerability	Potential Vulnerability - level 3	
12826	EMC Documentum eRoom Indexing Server Remote Buffer Overflow Vulnerability (ESA-2011-022)	Potential Vulnerability - level 3	Practice
12826	Novell Evolution Unspecified Denial of Service Vulnerability	Potential Vulnerability - level 3	
12838	Moodle Information Disclosure and Unauthorized Content Modification Vulnerabilities	Vulnerability - level 3	Vuln
12838	Sun Solaris NewGRP Local Buffer Overflow Vulnerability	Vulnerability - level 3	
12840	Avaya Voice Portal Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
12840	Massimiliano Montoro Cain & Abel PSK Sniffer Remote Heap Buffer Overflow Vulnerability	Potential Vulnerability - level 4	
12853	PHP-Fusion Setuser.PHP HTML Injection Vulnerability	Potential Vulnerability - level 4	
12853	Ruby on Rails Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
12888	Invision Power Board HTML Injection Vulnerability	Vulnerability - level 4	
12888	Moodle Versions Prior to 2.6.2, 2.5.5 and 2.4.9 Multiple Vulnerabilities	Vulnerability - level 4	Vuln
12930	CPG Dragonfly Multiple Cross-Site Scripting Vulnerabilities	Potential Vulnerability - level 4	
12930	Splunk OpenSSL Multiple Vulnerabilities (Heartbleed Bug)	Potential Vulnerability - level 4	Practice
13046	Mozilla Bugzilla Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
13046	Ocean12 Membership Manager Pro Cross-Site Scripting Vulnerability	Potential Vulnerability - level 4	
13264	Nginx Heap-Based Buffer Overflow Vulnerability	Potential Vulnerability - level 3	Practice
13264	RealNetworks RealPlayer Enterprise Unspecified RAM File Processing Buffer Overflow Vulnerability	Potential Vulnerability - level 3	
13267	Linux Kernel Fib_Seq_Start Local Denial of Service Vulnerability	Potential Vulnerability - level 3	
13267	Nginx STARTTLS Command Injection Vulnerability	Potential Vulnerability - level 3	Practice
13331	Atlassian Hipchat Integration Plugin for Bitbucket Server, Jira, Confluence Secret Key Vulnerability	Potential Vulnerability - level 4	Practice
13331	CartWIZ ProductCatalogSubCats.ASP SQL Injection Vulnerability	Potential Vulnerability - level 4	
13335	Advantech WebAccess Multiple Security Vulnerabilities	Vulnerability - level 4	Vuln
13335	CartWIZ SearchResults.ASP IDCategory Argument SQL Injection Vulnerability	Vulnerability - level 4	
13407	Advantech WebAccess Multiple Security Vulnerabilities	Vulnerability - level 4	Vuln
13407	Claroline E-Learning Application Multiple Remote Input Validation Vulnerabilities	Vulnerability - level 4	
13460	Advantech WebAccess Multiple Security Vulnerabilities	Vulnerability - level 4	Vuln
13460	Mtp-Target Client Remote Format String Vulnerability	Vulnerability - level 4	
13474	Drupal Core Multiple Vulnerabilities(SA-CORE-2019-006)	Vulnerability - level 4	Vuln

13474	SmartList ListManager Arbitrary List Addition Vulnerability	Vulnerability - level 4	
13481	SitePanel2 Multiple Input Validation Vulnerabilities	Potential Vulnerability - level 3	
13481	jQuery Prior to 3.4.0 Cross-Site Scripting Vulnerability	Potential Vulnerability - level 3	Practice
13534	Invision Power Board Topics.PHP Highlite Parameter Cross-Site Scripting Vulnerability	Potential Vulnerability - level 4	
13534	Wind River VxWorks Multiple Security Vulnerabilities(URGENT 11)	Potential Vulnerability - level 4	Practice
13678	Joomla! Core JQuery extend Cross-Site Scripting Vulnerability [20190403]	Vulnerability - level 3	Vuln
13678	Novell ZENworks Multiple Remote Pre-Authentication Memory Corruption Vulnerabilities	Vulnerability - level 3	
13679	D-Link DSL Router Remote Authentication Bypass Vulnerability	Vulnerability - level 4	
13679	Nortek Linear eMerge Multiple Vulnerabilities	Vulnerability - level 4	Vuln
13784	Node.js Multiple Security Vulnerabilities (June-2020)	Vulnerability - level 4	Vuln
13784	Nokia 9500 vCard Viewer Remote Denial of Service Vulnerability	Vulnerability - level 4	
13788	Hummingbird Connectivity 10 LPD Daemon Stack Overflow Vulnerability	Vulnerability - level 4	
13788	Palo Alto Networks PAN-OS:OpenSSH Software Vulnerabilities(PAN-SA-2020-0005,PAN-111061)	Vulnerability - level 4	Vuln
13790	Hummingbird Connectivity 10 FTP Daemon Heap Overflow Vulnerability	Vulnerability - level 4	
13790	Palo Alto Networks (PAN-OS) Open Secure Sockets Layer (OpenSSL) Vulnerabilities (PAN-98504 PAN-SA-2018-0015)	Vulnerability - level 4	Vuln
150398	Apache HTTP Server Multiple Vulnerabilities(CVE-2021-26690,CVE-2021-26691)	Potential Vulnerability - level 3	Practice
150399	Apache HTTP Server Multiple Vulnerabilities (CVE-2021-34798,CVE-2021-39275)	Potential Vulnerability - level 3	Practice
150515	Apache HTTP Server Prior to 2.4.53 Multiple Security Vulnerabilities	Potential Vulnerability - level 5	Practice
150539	Apache HTTP Server Prior to 2.4.54 Multiple Security Vulnerabilities	Potential Vulnerability - level 4	Practice
15056	ISC BIND DNSSEC Additional Section Cache Poisoning Vulnerability	Potential Vulnerability - level 2	Practice
15056	Microsoft Windows MSDTC Buffer Overflow Vulnerability	Potential Vulnerability - level 2	
15057	ISC BIND 9 DNSSEC Bogus NXDOMAIN Response Remote Cache Poisoning Vulnerability	Potential Vulnerability - level 3	Practice
15057	Microsoft MSDTC COM+ Remote Code Execution Vulnerability	Potential Vulnerability - level 3	
15059	ISC BIND Denial of Service and Security Bypass Vulnerabilities	Potential Vulnerability - level 2	Practice
15059	Microsoft MSDTC TIP Distributed Denial Of Service Vulnerability	Potential Vulnerability - level 2	
15061	ISC BIND Key Algorithm Rollover Weakness Vulnerability	Potential Vulnerability - level 2	Practice
15061	Microsoft Internet Explorer COM Object Instantiation Variant Vulnerability	Potential Vulnerability - level 2	
15062	ISC BIND RRSIG / ncache Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
15062	RARLAB WinRAR Multiple Remote Vulnerabilities	Potential Vulnerability - level 3	
15082	ISC BIND 9 Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
15082	Zope RestructuredText Unspecified Security Vulnerability	Potential Vulnerability - level 3	
15085	ISC BIND DNSSEC Validation Remote Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice

15085	Linux Orinoco Driver Remote Information Disclosure Vulnerability	Potential Vulnerability - level 3	
15089	ISC BIND 9.6-ESV-R9-P1 Not Installed	Potential Vulnerability - level 3	Practice
15092	ISC BIND Recursive Nameservers Remote Denial of Service Vulnerability	Vulnerability - level 4	Practice
15092	Yapig View.PHP Cross-Site Scripting Vulnerability	Vulnerability - level 4	
15093	Hitachi OpenTP1 Denial Of Service Vulnerability	Vulnerability - level 3	
15093	ISC BIND EDNS Option Processing Denial of Service Vulnerability	Vulnerability - level 3	Practice
15094	ISC BIND GeoIP Feature Processing Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
15094	Kerio Personal Firewall and ServerFirewall Local Denial of Service Vulnerability	Potential Vulnerability - level 3	
151015	Vulnerable JavaScript Library Detected - jQuery	Vulnerability - level 3	Vuln
151025	Vulnerable JavaScript Library Detected - Moment.js	Vulnerability - level 3	Vuln
15123	ISC BIND Buffer Overflow Vulnerability	Potential Vulnerability - level 4	Practice
15123	RARLAB WinRAR Command Line Processing Buffer Overflow Vulnerability	Potential Vulnerability - level 4	
15124	ISC BIND Buffer Overflow Vulnerability	Potential Vulnerability - level 4	Practice
15124	Opera Web Browser Multiple Malformed HTML Parsing Denial Of Service Vulnerabilities	Potential Vulnerability - level 4	
15125	E107 Resetcore.PHP SQL Injection Vulnerability	Potential Vulnerability - level 3	
15125	ISC BIND Broken Inbound Incremental Zone Update Vulnerability	Potential Vulnerability - level 3	Practice
15126	IBM DB2 Universal Database Multiple Vulnerabilities	Potential Vulnerability - level 4	
15126	ISC BIND Assertion Failure Vulnerability	Potential Vulnerability - level 4	Practice
15128	ISC BIND Lame cache Vulnerability	Potential Vulnerability - level 3	Practice
15128	NetPBM PNMTOPNG Buffer Overflow Vulnerability	Potential Vulnerability - level 3	
15129	ISC BIND Domain Name System (DNS) forwarders - cache poisoning Vulnerability	Potential Vulnerability - level 4	Practice
15129	Rockliffe MailSite Express Arbitrary File Upload Vulnerability	Potential Vulnerability - level 4	
15130	ISC BIND Denial of Service (DoS) Vulnerability	Potential Vulnerability - level 3	Practice
15130	Microsoft Windows Unspecified Remote Code Execution Vulnerability	Potential Vulnerability - level 3	
154040	Drupal Core XSS Vulnerability (SA-CORE-2019-006)	Vulnerability - level 4	Vuln
155000	Oracle Enterprise Linux Security Update for tomcat (ELSA-2015-0983)	Vulnerability - level 3	Vuln
155015	Oracle Enterprise Linux xterm Security Update (ELSA-2009-0018)	Vulnerability - level 2	Vuln
155019	Oracle Enterprise Linux squirrelmail Security Update (ELSA-2009-0010)	Vulnerability - level 2	Vuln
155025	Oracle Enterprise Linux enscript Security Update (ELSA-2008-1016)	Vulnerability - level 2	Vuln
155027	Oracle Enterprise Linux enscript Security Update (ELSA-2008-1021)	Vulnerability - level 2	Vuln
155032	Oracle Enterprise Linux kernel Security and Bug Fix Update (ELSA-2008-0973)	Vulnerability - level 2	Vuln
155037	Oracle Enterprise Linux httpd Security and Bug Fix Update (ELSA-2008-0967)	Vulnerability - level 2	Vuln
155050	Oracle Enterprise Linux pam_krb5 Security Update (ELSA-2008-0907)	Vulnerability - level 2	Vuln

155062	Oracle Enterprise Linux Kernel Security and Bug Fix Update (ELSA-2008-0612)	Vulnerability - level 2	Vuln
155073	Oracle Enterprise Linux Seamonkey Security Update (ELSA-2008-0547)	Vulnerability - level 2	Vuln
155074	Oracle Enterprise Linux Firefox Security Update (ELSA-2008-0549)	Vulnerability - level 2	Vuln
155075	Oracle Enterprise Linux Firefox Security Update (ELSA-2008-0569)	Vulnerability - level 2	Vuln
155077	Oracle Enterprise Linux Pidgin Security and Bug Fix Update (ELSA-2008-0584)	Vulnerability - level 2	Vuln
155082	Oracle Enterprise Linux php Security Update (ELSA-2008-0544)	Vulnerability - level 2	Vuln
155083	Oracle Enterprise Linux php Security and Bug Fix Update (ELSA-2008-0545)	Vulnerability - level 2	Vuln
155087	Oracle Enterprise Linux Kernel Security and Bug Fix Update (ELSA-2008-0607)	Vulnerability - level 2	Vuln
155088	Oracle Enterprise Linux Thunderbird Security Update (ELSA-2008-0616)	Vulnerability - level 2	Vuln
155103	Oracle Enterprise Linux freetype Security Update (ELSA-2008-0556)	Vulnerability - level 2	Vuln
155104	Oracle Enterprise Linux Security Update for tomcat6 (ELSA-2015-0991)	Vulnerability - level 3	Vuln
155108	Oracle Enterprise Linux Kernel Security and Bug Fix Update (ELSA-2008-0237)	Vulnerability - level 2	Vuln
155116	Oracle Enterprise Linux kernel Security and Bug Fix Update (ELSA-2008-0275)	Vulnerability - level 2	Vuln
155135	Oracle Enterprise Linux Tomcat Security Update (ELSA-2008-0042)	Vulnerability - level 2	Vuln
155137	Oracle Enterprise Linux krb5 Security Update (ELSA-2008-0180)	Vulnerability - level 2	Vuln
155138	Oracle Enterprise Linux krb5 Security Update (ELSA-2008-0181)	Vulnerability - level 2	Vuln
155139	Oracle Enterprise Linux unzip Security Update (ELSA-2008-0196)	Vulnerability - level 2	Vuln
155140	Oracle Enterprise Linux krb5 Security and Bug Fix Update (ELSA-2008-0164)	Vulnerability - level 5	Vuln
155150	Oracle Enterprise Linux tk Security Update (ELSA-2008-0136)	Vulnerability - level 2	Vuln
155151	Oracle Enterprise Linux tcltk Security Update (ELSA-2008-0134)	Vulnerability - level 2	Vuln
155152	Oracle Enterprise Linux tk Security Update (ELSA-2008-0135)	Vulnerability - level 2	Vuln
155164	Oracle Enterprise Linux httpd Security Update (ELSA-2008-0005)	Vulnerability - level 2	Vuln
155165	Oracle Enterprise Linux httpd Security Update (ELSA-2008-0006)	Vulnerability - level 2	Vuln
155166	Oracle Enterprise Linux httpd Security Update (ELSA-2008-0008)	Vulnerability - level 2	Vuln
155177	Oracle Enterprise Linux util-linux Security Update (ELSA-2007-0969)	Vulnerability - level 2	Vuln
155178	Oracle Enterprise Linux Critical: Samba Security Update (ELSA-2007-1016)	Vulnerability - level 2	Vuln
155179	Oracle Enterprise Linux net-snmp Security Update (ELSA-2007-1045)	Vulnerability - level 2	Vuln
155196	Oracle Enterprise Linux perl Security Update (ELSA-2007-0966)	Vulnerability - level 2	Vuln
155212	Oracle Enterprise Linux Security Update for openssl (ELSA-2015-0800)	Vulnerability - level 3	Vuln
155226	Oracle Enterprise Linux Security Update for openssl (ELSA-2015-1072)	Vulnerability - level 3	Vuln
155233	Oracle Enterprise Linux Security Update for wpa_supplicant (ELSA-2015-1090)	Vulnerability - level 3	Vuln
155234	Oracle Enterprise Linux Security Update for openssl (ELSA-2015-1115)	Vulnerability - level 3	Vuln
155243	Oracle Enterprise Linux Security Update for nss (ELSA-2015-1185)	Vulnerability - level 3	Vuln
155247	Oracle Enterprise Linux Security Update for openssl (ELSA-2015-1197)	Vulnerability - level 3	Vuln
155253	Oracle Enterprise Linux Security Update for java-1.8.0-openjdk (ELSA-2015-1228)	Vulnerability - level 4	Vuln
155254	Oracle Enterprise Linux Security Update for java-1.7.0-openjdk (ELSA-2015-1229)	Vulnerability - level 5	Vuln
155257	Oracle Enterprise Linux Security Update for java-1.7.0-openjdk (ELSA-2015-1230)	Vulnerability - level 4	Vuln

155269	Oracle Enterprise Linux Security Update for curl (ELSA-2015-1254)	Vulnerability - level 3	Vuln
155280	Oracle Enterprise Linux Security Update for ntp (ELSA-2015-1459)	Vulnerability - level 3	Vuln
155287	Oracle Enterprise Linux Security Update for java-1.6.0-openjdk (ELSA-2015-1526)	Vulnerability - level 4	Vuln
155303	Oracle Enterprise Linux Security Update for subversion (ELSA-2015-1633)	Vulnerability - level 3	Vuln
155317	Oracle Enterprise Linux Security Update for subversion (ELSA-2015-1742)	Vulnerability - level 3	Vuln
155335	Oracle Enterprise Linux Security Update for ntp (ELSA-2015-1930)	Vulnerability - level 3	Vuln
155358	Oracle Enterprise Linux openssl Security Update (ELSA-2006:0661, ELSA-2006:0695)	Vulnerability - level 4	Vuln
155365	Oracle Enterprise Linux Security Update for openssh (ELSA-2015-2088)	Vulnerability - level 3	Vuln
155369	Oracle Enterprise Linux Security Update for curl (ELSA-2015-2159)	Vulnerability - level 3	Vuln
155377	Oracle Enterprise Linux Security Update for ntp (ELSA-2015-2231)	Vulnerability - level 3	Vuln
155378	Oracle Enterprise Linux Security Update for unbound (ELSA-2015-2455)	Vulnerability - level 3	Vuln
155402	Oracle Enterprise Linux 5 Glibc Security Update (ELSA-2011-0412)	Vulnerability - level 3	Vuln
155408	Oracle Enterprise Linux 5 Tomcat5 Security Update (ELSA-2010-0580)	Vulnerability - level 3	Vuln
155409	Oracle Enterprise Linux Update for glibc (ELSA-2011-0413)	Vulnerability - level 4	Vuln
155411	Oracle Enterprise Linux Update for kernel (ELSA-2011-0421)	Vulnerability - level 4	Vuln
155414	Oracle Enterprise Linux Update for kernel (ELSA-2011-0429)	Vulnerability - level 4	Vuln
155428	Oracle Enterprise Linux Update for Unbreakable Enterprise Kernel (ELSA-2011-2014)	Vulnerability - level 5	Vuln
155438	Oracle Enterprise Linux Update for GIMP (ELSA-2011-0837)	Vulnerability - level 3	Vuln
155439	Oracle Enterprise Linux Update for GIMP (ELSA-2011-0838)	Vulnerability - level 3	Vuln
155441	Oracle Enterprise Linux Update for Postfix (ELSA-2011-0843)	Vulnerability - level 3	Vuln
155445	Oracle Enterprise Linux Update for Unbreakable Enterprise Kernel (ELSA-2011-2016)	Vulnerability - level 3	Vuln
155446	Oracle Enterprise Linux Update for Kernel (ELSA-2011-0007)	Vulnerability - level 4	Vuln
155448	Oracle Enterprise Linux Update for Kernel (ELSA-2011-0303)	Vulnerability - level 3	Vuln
155465	Oracle Enterprise Linux Update for tomcat6 (ELSA-2011-0335)	Vulnerability - level 4	Vuln
155480	Oracle Enterprise Linux Update for libtiff (ELSA-2011-0392)	Vulnerability - level 4	Vuln
155486	Oracle Enterprise Linux Update for bzip2 (ELSA-2010-0858)	Vulnerability - level 4	Vuln
155494	Oracle Enterprise Linux Update for PAM (ELSA-2010-0891)	Vulnerability - level 3	Vuln
155503	Oracle Enterprise Linux Update for BIND (ELSA-2010-0975)	Vulnerability - level 4	Vuln
155504	Oracle Enterprise Linux Update for OpenSSL (ELSA-2010-0979)	Vulnerability - level 3	Vuln
155511	Oracle Enterprise Linux Update for Kernel (ELSA-2011-0163)	Vulnerability - level 4	Vuln
155521	Oracle Enterprise Linux Update for krb5 (ELSA-2011-0199)	Vulnerability - level 4	Vuln
155522	Oracle Enterprise Linux Update for krb5 (ELSA-2011-0200)	Vulnerability - level 4	Vuln
155530	Oracle Enterprise Linux Update for Oracle Enterprise Linux 4.9 Kernel (ELSA-2011-0263)	Vulnerability - level 4	Vuln
155532	Oracle Enterprise Linux Update for Kernel (ELSA-2011-0833)	Vulnerability - level 4	Vuln
155552	Oracle Enterprise Linux Update for Kernel Security, Bug Fix, and Enhancement Update (ELSA-2011-0004)	Vulnerability - level 4	Vuln
155554	Oracle Enterprise Linux Update for Kernel (ELSA-2011-0162)	Vulnerability - level 4	Vuln
155559	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0936)	Vulnerability - level 4	Vuln
155563	Oracle Enterprise Linux Update for BIND (ELSA-2010-0976)	Vulnerability - level 4	Vuln
155564	Oracle Enterprise Linux Update for OpenSSL (ELSA-2010-0977)	Vulnerability - level 3	Vuln
155565	Oracle Enterprise Linux Update for OpenSSL (ELSA-2010-0978)	Vulnerability - level 3	Vuln
155568	Oracle Enterprise Linux Update for BIND (ELSA-2010-1000)	Vulnerability - level 4	Vuln
155569	Oracle Linux 5 Unbreakable Enterprise Kernel Security and Bug Fix Update (ELSA-2010-2011)	Vulnerability - level 3	Vuln
155570	Oracle Enterprise Linux Update for PAM (ELSA-2010-0819)	Vulnerability - level 3	Vuln
155573	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0839)	Vulnerability - level 3	Vuln
155576	Oracle Enterprise Linux Update for krb5 (ELSA-2010-0926)	Vulnerability - level 3	Vuln
155587	Oracle Enterprise Linux Update for java-1.6.0-openjdk (ELSA-2010-0768)	Vulnerability - level 4	Vuln

155588	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0779)	Vulnerability - level 3	Vuln
155602	Oracle Enterprise Linux Update for Unbreakable Enterprise Kernel (ELSA-2010-2008)	Vulnerability - level 3	Vuln
155607	Oracle Enterprise Linux Update for RPM (ELSA-2010-0678)	Vulnerability - level 3	Vuln
155608	Oracle Enterprise Linux Update for RPM (ELSA-2010-0679)	Vulnerability - level 3	Vuln
155614	Oracle Enterprise Linux Update for bzip2 (ELSA-2010-0703)	Vulnerability - level 4	Vuln
155617	Oracle Enterprise Linux Update for mikmod (ELSA-2010-0720)	Vulnerability - level 3	Vuln
155618	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0723)	Vulnerability - level 4	Vuln
155621	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0606)	Vulnerability - level 4	Vuln
155623	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0610)	Vulnerability - level 4	Vuln
155633	Oracle Enterprise Linux Update for HTTP (ELSA-2010-0659)	Vulnerability - level 3	Vuln
155635	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0504)	Vulnerability - level 4	Vuln
155638	Oracle Enterprise Linux Update for libtiff (ELSA-2010-0519)	Vulnerability - level 4	Vuln
155639	Oracle Enterprise Linux Update for libtiff (ELSA-2010-0520)	Vulnerability - level 4	Vuln
155643	Oracle Enterprise Linux Update for Thunderbird (ELSA-2010-0544)	Vulnerability - level 3	Vuln
155656	Oracle Enterprise Linux Update for Kernel Security, Bug Fix, and Enhancement Update (ELSA-2010-0394)	Vulnerability - level 4	Vuln
155657	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0398)	Vulnerability - level 4	Vuln
155658	Oracle Enterprise Linux Update for teTeX (ELSA-2010-0399)	Vulnerability - level 3	Vuln
155659	Oracle Enterprise Linux Update for teTeX (ELSA-2010-0400)	Vulnerability - level 3	Vuln
155661	Oracle Enterprise Linux Update for krb5 (ELSA-2010-0423)	Vulnerability - level 4	Vuln
155667	Oracle Enterprise Linux Update for Firefox (ELSA-2010-0332)	Vulnerability - level 5	Vuln
155668	Oracle Enterprise Linux Update for Java-1.6.0-openjdk (ELSA-2010-0339)	Vulnerability - level 4	Vuln
155669	Oracle Enterprise Linux Update for krb5 (ELSA-2010-0343)	Vulnerability - level 4	Vuln
155671	Oracle Enterprise Linux Update for kdbase (ELSA-2010-0348)	Vulnerability - level 4	Vuln
155686	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0146)	Vulnerability - level 4	Vuln
155687	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0147)	Vulnerability - level 4	Vuln
155688	Oracle Enterprise Linux Update for Thunderbird (ELSA-2010-0154)	Vulnerability - level 3	Vuln
155689	Oracle Enterprise Linux Update for OpenSSL (ELSA-2010-0162)	Vulnerability - level 4	Vuln
155695	Oracle Enterprise Linux Update for OpenSSL 096b (ELSA-2010-0173)	Vulnerability - level 4	Vuln
155697	Oracle Enterprise Linux Update for cURL (ELSA-2010-0329)	Vulnerability - level 3	Vuln
155698	Oracle Enterprise Linux Update for SeaMonkey (ELSA-2010-0333)	Vulnerability - level 5	Vuln
155699	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0076)	Vulnerability - level 4	Vuln
155701	Oracle Enterprise Linux Update for HelixPlayer (ELSA-2010-0094)	Vulnerability - level 5	Vuln
155702	Oracle Enterprise Linux Update for OpenOffice.org (ELSA-2010-0101)	Vulnerability - level 4	Vuln
155705	Oracle Enterprise Linux Update for MySQL (ELSA-2010-0110)	Vulnerability - level 3	Vuln
155706	Oracle Enterprise Linux Update for Firefox (ELSA-2010-0112)	Vulnerability - level 5	Vuln
155707	Oracle Enterprise Linux Update for SeaMonkey (ELSA-2010-0113)	Vulnerability - level 5	Vuln
155712	Oracle Enterprise Linux Update for krb5-appl (ELSA-2011-0920)	Vulnerability - level 4	Vuln
155729	Oracle Enterprise Linux Update for gd (ELSA-2010-0003)	Vulnerability - level 3	Vuln
155735	Oracle Enterprise Linux Update for PHP (ELSA-2010-0040)	Vulnerability - level 3	Vuln
155737	Oracle Enterprise Linux Update for Kernel (ELSA-2010-0046)	Vulnerability - level 4	Vuln
155765	Oracle Enterprise Linux Update for BIND (ELSA-2009-1620)	Vulnerability - level 3	Vuln
155783	Oracle Enterprise Linux Update for OpenOffice.org (ELSA-2009-1426)	Vulnerability - level 4	Vuln
155785	Oracle Enterprise Linux Update for xmlsec1 (ELSA-2009-1428)	Vulnerability - level 3	Vuln
155805	Oracle Enterprise Linux Update for DHCP (ELSA-2011-1160)	Vulnerability - level 3	Vuln
155820	Oracle Enterprise Linux Update for Kernel (ELSA-2009-1193)	Vulnerability - level 4	Vuln
155821	Oracle Enterprise Linux Update for java-1.6.0-openjdk (ELSA-2009-1201)	Vulnerability - level 4	Vuln
155822	Oracle Enterprise Linux Update for Subversion (ELSA-2009-1203)	Vulnerability - level 4	Vuln
155843	Oracle Enterprise Linux Update for libtiff (ELSA-2009-1159)	Vulnerability - level 3	Vuln
155846	Oracle Enterprise Linux Update for Tomcat (ELSA-2009-1164)	Vulnerability - level 4	Vuln
155906	Oracle Enterprise Linux Update for FreeType (ELSA-2009-0329)	Vulnerability - level 4	Vuln
155912	Oracle Enterprise Linux Update for Poppler (ELSA-2009-0480)	Vulnerability - level 4	Vuln
155925	Oracle Enterprise Linux Update for krb5 (ELSA-2009-0408)	Vulnerability - level 4	Vuln

155926	Oracle Enterprise Linux Update for krb5 (ELSA-2009-0409)	Vulnerability - level 4	Vuln
155927	Oracle Enterprise Linux Update for krb5 (ELSA-2009-0410)	Vulnerability - level 5	Vuln
155933	Oracle Enterprise Linux Update for CUPS (ELSA-2009-0429)	Vulnerability - level 4	Vuln
155934	Oracle Enterprise Linux Update for Xpdf (ELSA-2009-0430)	Vulnerability - level 4	Vuln
155935	Oracle Enterprise Linux Update for kdegraphics (ELSA-2009-0431)	Vulnerability - level 4	Vuln
155941	Oracle Enterprise Linux Update for GPDF (ELSA-2009-0458)	Vulnerability - level 4	Vuln
155964	Oracle Enterprise Linux Update for Openswan (ELSA-2009-0402)	Vulnerability - level 4	Vuln
155991	Oracle Enterprise Linux Update for Samba (ELSA-2007-1013)	Vulnerability - level 5	Vuln
156017	Oracle Enterprise Linux Update for Kernel (ELSA-2011-1465)	Vulnerability - level 4	Vuln
156020	Oracle Enterprise Linux Update for Unbreakable Enterprise Kernel (ELSA-2011-2033)	Vulnerability - level 3	Vuln
156022	Oracle Enterprise Linux Update for OpenSSL (ELSA-2007-0813)	Vulnerability - level 3	Vuln
156029	Oracle Enterprise Linux Update for OpenSSL (ELSA-2007-0964)	Vulnerability - level 5	Vuln
156040	Oracle Enterprise Linux Update for Cyrus-sasl (ELSA-2007-0795)	Vulnerability - level 3	Vuln
156043	Oracle Enterprise Linux Update for Krb5 (ELSA-2007-0858)	Vulnerability - level 5	Vuln
156046	Oracle Enterprise Linux Update for Cyrus-sasl (ELSA-2007-0878)	Vulnerability - level 3	Vuln
156064	Oracle Enterprise Linux Update for Tomcat (ELSA-2007-0569)	Vulnerability - level 3	Vuln
156089	Oracle Enterprise Linux Update for Tomcat (ELSA-2007-0327)	Vulnerability - level 4	Vuln
156117	Oracle Enterprise Linux Update for gcc (ELSA-2007-0473)	Vulnerability - level 3	Vuln
156143	Oracle Enterprise Linux Update for Tomcat5 (ELSA-2011-1845)	Vulnerability - level 3	Vuln
156147	Oracle Enterprise Linux Update for Unbreakable Enterprise Kernel (ELSA-2011-2037)	Vulnerability - level 3	Vuln
156150	Oracle Enterprise Linux Update for unzip (ELSA-2007-0203)	Vulnerability - level 2	Vuln
156152	Oracle Enterprise Linux Update for gcc (ELSA-2007-0220)	Vulnerability - level 3	Vuln
156183	Oracle Enterprise Linux Update for Samba (ELSA-2007:0060)	Vulnerability - level 3	Vuln
156202	Oracle Enterprise Linux Update for Texinfo (ELSA-2006:0727)	Vulnerability - level 3	Vuln
156223	Oracle Enterprise Linux Update for t1lib (ELSA-2012-0062)	Vulnerability - level 3	Vuln
156265	Oracle Enterprise Linux Update for TeX Live (ELSA-2012-0137)	Vulnerability - level 5	Vuln
156284	Oracle Enterprise Linux Update for krb5 (ELSA-2012-0306)	Vulnerability - level 3	Vuln
156303	Oracle Enterprise Linux Update for Raptor (ELSA-2012-0410)	Vulnerability - level 4	Vuln
156340	Oracle Enterprise Linux Update for OpenOffice.org (ELSA-2012-0705)	Vulnerability - level 4	Vuln
156387	Oracle Enterprise Linux Update for glibc (ELSA-2012-1097)	Vulnerability - level 3	Vuln
156388	Oracle Enterprise Linux Update for glibc (ELSA-2012-1098)	Vulnerability - level 3	Vuln
156400	Oracle Enterprise Linux Update for libreoffice (ELSA-2012-1135)	Vulnerability - level 4	Vuln
156409	Oracle Enterprise Linux Update for GIMP (ELSA-2012-1181)	Vulnerability - level 5	Vuln
156410	Oracle Enterprise Linux Update for teTeX (ELSA-2012-1201)	Vulnerability - level 3	Vuln
156415	Oracle Enterprise Linux Update for Firefox (ELSA-2012-1210)	Vulnerability - level 5	Vuln
156416	Oracle Enterprise Linux Update for Thunderbird (ELSA-2012-1211)	Vulnerability - level 5	Vuln
156417	Oracle Enterprise Linux Update for java-1.6.0-openjdk (ELSA-2012-1221)	Vulnerability - level 5	Vuln
156418	Oracle Enterprise Linux Update for java-1.6.0-openjdk (ELSA-2012-1222)	Vulnerability - level 5	Vuln
156419	Oracle Enterprise Linux Update for java-1.7.0-openjdk (ELSA-2012-1223)	Vulnerability - level 5	Vuln
156423	Oracle Enterprise Linux Update for libexif (ELSA-2012-1255)	Vulnerability - level 4	Vuln
156430	Oracle Enterprise Linux Update for libxslt (ELSA-2012-1265)	Vulnerability - level 3	Vuln
156439	Oracle Enterprise Linux Update for Kernel (ELSA-2012-1323)	Vulnerability - level 3	Vuln
156440	Oracle Enterprise Linux Update for FreeRADIUS (ELSA-2012-1326)	Vulnerability - level 3	Vuln
156441	Oracle Enterprise Linux Update for freeradius2 (ELSA-2012-1327)	Vulnerability - level 3	Vuln
156464	Oracle Enterprise Linux Update for libproxy (ELSA-2012-1461)	Vulnerability - level 3	Vuln
156476	Oracle Enterprise Linux Update for libtiff (ELSA-2012-1590)	Vulnerability - level 3	Vuln
156523	Oracle Enterprise Linux Update for java-1.6.0-openjdk (ELSA-2013-0273)	Vulnerability - level 5	Vuln
156524	Oracle Enterprise Linux Update for java-1.6.0-openjdk (ELSA-2013-0274)	Vulnerability - level 5	Vuln
156525	Oracle Enterprise Linux Update for java-1.7.0-openjdk (ELSA-2013-0275)	Vulnerability - level 5	Vuln
156555	Oracle Enterprise Linux Update for libxml2 (ELSA-2013-0581)	Vulnerability - level 3	Vuln

156559	Oracle Enterprise Linux Update for OpenSSL (ELSA-2013-0587)	Vulnerability - level 3	Vuln
156562	Oracle Enterprise Linux Update for nss-pam-ldapd (ELSA-2013-0590)	Vulnerability - level 3	Vuln
156571	Oracle Enterprise Linux Update for Ruby (ELSA-2013-0611)	Vulnerability - level 3	Vuln
156572	Oracle Enterprise Linux Update for Ruby (ELSA-2013-0612)	Vulnerability - level 3	Vuln
156573	Oracle Enterprise Linux Update for xulrunner (ELSA-2013-0614)	Vulnerability - level 3	Vuln
156575	Oracle Enterprise Linux Update for tomcat6 (ELSA-2013-0623)	Vulnerability - level 3	Vuln
156576	Oracle Enterprise Linux Update for Thunderbird (ELSA-2013-0627)	Vulnerability - level 3	Vuln
156579	Oracle Enterprise Linux Update for tomcat5 (ELSA-2013-0640)	Vulnerability - level 3	Vuln
156583	Oracle Enterprise Linux Update for SSSD (ELSA-2013-0663)	Vulnerability - level 3	Vuln
156585	Oracle Enterprise Linux Update for Perl (ELSA-2013-0685)	Vulnerability - level 4	Vuln
156587	Oracle Enterprise Linux Update for BIND (ELSA-2013-0689)	Vulnerability - level 3	Vuln
156588	Oracle Enterprise Linux Update for bind97 (ELSA-2013-0690)	Vulnerability - level 3	Vuln
156593	Oracle Enterprise Linux Update for KVM (ELSA-2013-0727)	Vulnerability - level 4	Vuln
156594	Oracle Enterprise Linux Update for Subversion (ELSA-2013-0737)	Vulnerability - level 3	Vuln
156597	Oracle Enterprise Linux Update for Kernel (ELSA-2013-0744)	Vulnerability - level 4	Vuln
156599	Oracle Enterprise Linux Update for java-1.7.0-openjdk (ELSA-2013-0751)	Vulnerability - level 5	Vuln
156600	Oracle Enterprise Linux Update for java-1.7.0-openjdk (ELSA-2013-0752)	Vulnerability - level 5	Vuln
156602	Oracle Enterprise Linux Update for java-1.6.0-openjdk (ELSA-2013-0770)	Vulnerability - level 5	Vuln
156606	Oracle Enterprise Linux Update for Unbreakable Enterprise Kernel (ELSA-2013-2519)	Vulnerability - level 3	Vuln
156607	Oracle Enterprise Linux Update for Unbreakable Enterprise Kernel (ELSA-2013-2520)	Vulnerability - level 4	Vuln
156609	Oracle Enterprise Linux Update for httpd (ELSA-2013-0815)	Vulnerability - level 3	Vuln
156619	Oracle Enterprise Linux Update for libvirt (ELSA-2013-0831)	Vulnerability - level 3	Vuln
156628	Oracle Enterprise Linux Update for tomcat6 (ELSA-2013-0964)	Vulnerability - level 3	Vuln
156635	Oracle Enterprise Linux Update for krb5 (ELSA-2013-0942)	Vulnerability - level 3	Vuln
156642	Oracle Enterprise Linux Security Update for Ruby (ELSA-2013-1090)	Vulnerability - level 3	Vuln
156673	Oracle Enterprise Linux Security Update for Unbreakable Enterprise Kernel (ELSA-2013-2543)	Vulnerability - level 3	Vuln
156676	Oracle Enterprise Linux Security Update for gdm (ELSA-2013-1213)	Vulnerability - level 4	Vuln
156689	Oracle Enterprise Linux Security Update for php53 (ELSA-2013-1307)	Vulnerability - level 4	Vuln
156692	Oracle Enterprise Linux Security Update for samba3x (ELSA-2013-1310)	Vulnerability - level 3	Vuln
156698	Oracle Enterprise Linux Security Update for rubygems (ELSA-2013-1441)	Vulnerability - level 3	Vuln
156706	Oracle Enterprise Linux Security Update for gnupg2 (ELSA-2013-1459)	Vulnerability - level 3	Vuln
156708	Oracle Enterprise Linux Security Update for gnupg (ELSA-2013-1458)	Vulnerability - level 3	Vuln
156710	Oracle Enterprise Linux Security Update for postgresql and postgresql84 (ELSA-2013-1475)	Vulnerability - level 3	Vuln
156717	Oracle Enterprise Linux Security Update for Samba (ELSA-2013-1542)	Vulnerability - level 3	Vuln
156720	Oracle Enterprise Linux Security Update for PHP (ELSA-2013-1615)	Vulnerability - level 3	Vuln
156722	Oracle Enterprise Linux Security Update for Kernel (ELSA-2013-1645)	Vulnerability - level 4	Vuln
156726	Oracle Enterprise Linux Security Update for 389-ds-base (ELSA-2013-1752)	Vulnerability - level 4	Vuln
156731	Oracle Enterprise Linux Security Update for xorg-x11-server (ELSA-2013-1620)	Vulnerability - level 2	Vuln
156740	Oracle Enterprise Linux Security Update for mod_nss (ELSA-2013-1779)	Vulnerability - level 3	Vuln

156743	Oracle Enterprise Linux Security Update for libjpeg-turbo (ELSA-2013-1803)	Vulnerability - level 3	Vuln
156746	Oracle Enterprise Linux Security Update for libjpeg (ELSA-2013-1804)	Vulnerability - level 3	Vuln
156748	Oracle Enterprise Linux Security Update for PHP (ELSA-2013-1814)	Vulnerability - level 5	Vuln
156764	Oracle Enterprise Linux Security Update for OpenSSL (ELSA-2014-0015)	Vulnerability - level 4	Vuln
156765	Oracle Enterprise Linux Security Update for gnupg (ELSA-2014-0016)	Vulnerability - level 3	Vuln
156783	Oracle Enterprise Linux Security Update for mysql (ELSA-2014-0164)	Vulnerability - level 3	Vuln
156788	Oracle Enterprise Linux Security Update for openswan (ELSA-2014-0185)	Vulnerability - level 3	Vuln
156789	Oracle Enterprise Linux Security Update for mysql55-mysql (ELSA-2014-0186)	Vulnerability - level 3	Vuln
156792	Oracle Enterprise Linux Security Update for libtiff (ELSA-2014-0222, ELSA-2014-0223)	Vulnerability - level 3	Vuln
156793	Oracle Enterprise Linux Security Update for gnutls (ELSA-2014-0246)	Vulnerability - level 4	Vuln
156794	Oracle Enterprise Linux Security Update for gnutls (ELSA-2014-0247)	Vulnerability - level 4	Vuln
156796	Oracle Enterprise Linux Security Update for subversion (ELSA-2014-0255)	Vulnerability - level 3	Vuln
156798	Oracle Enterprise Linux Security Update for Kernel (ELSA-2014-0285)	Vulnerability - level 4	Vuln
156802	Oracle Enterprise Linux Security Update for samba (ELSA-2014-0305)	Vulnerability - level 3	Vuln
156808	Oracle Enterprise Linux Security Update for Kernel (ELSA-2014-0328)	Vulnerability - level 4	Vuln
156824	Oracle Enterprise Linux Security Update for tomcat6 (ELSA-2014-0429)	Vulnerability - level 3	Vuln
156832	Oracle Enterprise Linux Security Update for openssl (ELSA-2014-0625)	Vulnerability - level 4	Vuln
156844	Oracle Enterprise Linux Security Update for Kernel (ELSA-2014-0771)	Vulnerability - level 4	Vuln
156851	Oracle Enterprise Linux Security Update for tomcat6 (ELSA-2014-0865)	Vulnerability - level 3	Vuln
156866	Oracle Enterprise Linux Security Update for openssl (ELSA-2014-0679)	Vulnerability - level 4	Vuln
156870	Oracle Enterprise Linux Security Update for tomcat (ELSA-2014-0686)	Vulnerability - level 4	Vuln
156873	Oracle Enterprise Linux Security Update for json-c (ELSA-2014-0703)	Vulnerability - level 3	Vuln
156876	Oracle Enterprise Linux Security Update for tomcat (ELSA-2014-0827)	Vulnerability - level 3	Vuln
156897	Oracle Enterprise Linux Security Update for tomcat (ELSA-2014-1034)	Vulnerability - level 2	Vuln
156901	Oracle Enterprise Linux Security Update for tomcat6 (ELSA-2014-1038)	Vulnerability - level 2	Vuln
156902	Oracle Enterprise Linux Security Update for openssl (ELSA-2014-1052)	Vulnerability - level 3	Vuln
156903	Oracle Enterprise Linux Security Update for openssl (ELSA-2014-1053)	Vulnerability - level 3	Vuln
156909	Oracle Enterprise Linux Security Update for httpcomponents-client (ELSA-2014-1146)	Vulnerability - level 4	Vuln
156915	Oracle Enterprise Linux Security Update for jakarta-commons-httpclient (ELSA-2014-1166)	Vulnerability - level 4	Vuln
157007	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2014-3108)	Vulnerability - level 3	Vuln

157008	Oracle Enterprise Linux Security Update for jasper (ELSA-2014-2021)	Vulnerability - level 4	Vuln
157011	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2014-3106)	Vulnerability - level 3	Vuln
157019	Oracle Enterprise Linux Security Update for openssl (ELSA-2015-0066)	Vulnerability - level 3	Vuln
157036	Oracle Enterprise Linux Security Update for subversion (ELSA-2015-0166)	Vulnerability - level 3	Vuln
157044	Oracle Enterprise Linux Security Update for openssl (ELSA-2015-3010)	Vulnerability - level 3	Vuln
157060	Oracle Enterprise Linux Security Update for libreoffice (ELSA-2015-0377)	Vulnerability - level 3	Vuln
157068	Oracle Enterprise Linux Security Update for openssl (ELSA-2015-0716)	Vulnerability - level 3	Vuln
157069	Oracle Enterprise Linux Security Update for openssl (ELSA-2015-0715)	Vulnerability - level 3	Vuln
157083	Oracle Enterprise Linux Security Update for openssl (ELSA-2015-2617)	Vulnerability - level 3	Vuln
157085	Oracle Enterprise Linux Security Update for openssl (ELSA-2015-2616)	Vulnerability - level 3	Vuln
157114	Oracle Enterprise Linux Security Update for ntp (ELSA-2016-0063)	Vulnerability - level 3	Vuln
157143	Oracle Enterprise Linux Security Update for openssl (ELSA-2016-0302)	Vulnerability - level 4	Vuln
157147	Oracle Enterprise Linux Security Update for openssl098e (ELSA-2016-0372)	Vulnerability - level 4	Vuln
157151	Oracle Enterprise Linux Security Update for xerces-c (ELSA-2016-0430)	Vulnerability - level 4	Vuln
157152	Oracle Enterprise Linux Security Update for openssh (ELSA-2016-0465)	Vulnerability - level 3	Vuln
157178	Oracle Enterprise Linux Security Update for openssl (ELSA-2016-0722)	Vulnerability - level 3	Vuln
157185	Oracle Enterprise Linux Security Update for openssl (ELSA-2016-0996)	Vulnerability - level 3	Vuln
157186	Oracle Enterprise Linux Security Update for openssh (ELSA-2016-0741)	Vulnerability - level 3	Vuln
157189	Oracle Enterprise Linux Security Update for ntp (ELSA-2016-0780)	Vulnerability - level 3	Vuln
157198	Oracle Enterprise Linux Security Update for ntp (ELSA-2016-1141)	Vulnerability - level 3	Vuln
157201	Oracle Enterprise Linux Security Update for openssl (ELSA-2016-1137)	Vulnerability - level 4	Vuln
157211	Oracle Enterprise Linux Security Update for openssl (ELSA-2016-3576)	Vulnerability - level 4	Vuln
157220	Oracle Enterprise Linux Security Update for httpd (ELSA-2016-1422) (HTTPoxy)	Vulnerability - level 4	Vuln
157221	Oracle Enterprise Linux Security Update for httpd (ELSA-2016-1421) (HTTPoxy)	Vulnerability - level 4	Vuln
157231	Oracle Enterprise Linux Security Update for libtiff (ELSA-2016-1547)	Vulnerability - level 4	Vuln
157241	Oracle Enterprise Linux Security Update for php (ELSA-2016-1613)	Vulnerability - level 3	Vuln
157242	Oracle Enterprise Linux Security Update for php (ELSA-2016-1609)	Vulnerability - level 3	Vuln
157261	Oracle Enterprise Linux Security Update for openssl (ELSA-2016-1940)	Vulnerability - level 4	Vuln
157271	Oracle Enterprise Linux Security Update for tomcat (ELSA-2016-2046)	Vulnerability - level 4	Vuln
157272	Oracle Enterprise Linux Security Update for tomcat6 (ELSA-2016-2045)	Vulnerability - level 4	Vuln
157275	Oracle Enterprise Linux Security Update for openssl (ELSA-2016-3627)	Vulnerability - level 4	Vuln
157282	Oracle Enterprise Linux Security Update for ntp (ELSA-2016-2583)	Vulnerability - level 3	Vuln
157288	Oracle Enterprise Linux Security Update for curl (ELSA-2016-2575)	Vulnerability - level 3	Vuln

157297	Oracle Enterprise Linux Security Update for php (ELSA-2016-2598)	Vulnerability - level 3	Vuln
157298	Oracle Enterprise Linux Security Update for tomcat (ELSA-2016-2599)	Vulnerability - level 3	Vuln
157300	Oracle Enterprise Linux Security Update for openssh (ELSA-2016-2588)	Vulnerability - level 3	Vuln
157377	Oracle Enterprise Linux Security Update for ntp (ELSA-2017-0252)	Vulnerability - level 3	Vuln
157407	Oracle Enterprise Linux Security Update for openssh (ELSA-2017-0641)	Vulnerability - level 3	Vuln
157429	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2017-3539)	Vulnerability - level 3	Vuln
157446	Oracle Enterprise Linux Security Update for jasper (ELSA-2017-1208)	Vulnerability - level 4	Vuln
157450	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2017-3566)	Vulnerability - level 4	Vuln
157451	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2017-3567)	Vulnerability - level 4	Vuln
157495	Oracle Enterprise Linux Security Update for java-1.8.0-openjdk (ELSA-2017-1789)	Vulnerability - level 5	Vuln
157502	Oracle Enterprise Linux Security Update for pidgin (ELSA-2017-1854)	Vulnerability - level 3	Vuln
157514	Oracle Enterprise Linux Security Update for curl (ELSA-2017-2016)	Vulnerability - level 3	Vuln
157518	Oracle Enterprise Linux Security Update for openssh (ELSA-2017-2029)	Vulnerability - level 3	Vuln
157520	Oracle Enterprise Linux Security Update for tomcat (ELSA-2017-2247)	Vulnerability - level 2	Vuln
157529	Oracle Enterprise Linux Security Update for java-1.7.0-openjdk (ELSA-2017-2424)	Vulnerability - level 5	Vuln
157543	Oracle Enterprise Linux Security Update for mercurial (ELSA-2017-2489)	Vulnerability - level 4	Vuln
157547	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2017-3609)	Vulnerability - level 3	Vuln
157578	Oracle Enterprise Linux Security Update for wpa_supplicant (ELSA-2017-2907) (KRACK Attack)	Vulnerability - level 3	Vuln
157579	Oracle Enterprise Linux Security Update for wpa_supplicant (ELSA-2017-2911) (KRACK Attack)	Vulnerability - level 3	Vuln
157581	Oracle Enterprise Linux Security Update for kernel (ELSA-2017-2930-1)	Vulnerability - level 3	Vuln
157586	Oracle Enterprise Linux Security Update for ntp (ELSA-2017-3071)	Vulnerability - level 3	Vuln
157608	Oracle Enterprise Linux Security Update for java-1.7.0-openjdk (ELSA-2017-3392)	Vulnerability - level 3	Vuln
157651	Oracle Enterprise Linux Security Update for quagga (ELSA-2018-0377)	Vulnerability - level 3	Vuln
157679	Oracle Enterprise Linux Security Update for ntp (ELSA-2018-0855)	Vulnerability - level 3	Vuln
157680	Oracle Enterprise Linux Security Update for openssh (ELSA-2018-0980)	Vulnerability - level 3	Vuln
157768	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2018-4189)(SegmentSmack)	Vulnerability - level 4	Vuln
157777	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2018-4190) (SegmentSmack)	Vulnerability - level 3	Vuln
157781	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2018-4195)	Vulnerability - level 3	Vuln
157783	Oracle Enterprise Linux Security Update for kernel (ELSA-2018-2390)	Vulnerability - level 3	Vuln
157784	Oracle Enterprise Linux Security Update for kernel (ELSA-2018-2384)	Vulnerability - level 3	Vuln
157797	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2018-4216)	Vulnerability - level 3	Vuln
157805	Oracle Enterprise Linux Security Update for kernel (ELSA-2018-2748)	Vulnerability - level 3	Vuln

157823	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2018-4249)	Vulnerability - level 3	Vuln
157824	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2018-4248)	Vulnerability - level 3	Vuln
157844	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2018-3221)	Vulnerability - level 3	Vuln
157864	Oracle Enterprise Linux Security Update for wpa_supplicant (ELSA-2018-3107)	Vulnerability - level 3	Vuln
157867	Oracle Enterprise Linux Security Update for xerces-c (ELSA-2018-3335)	Vulnerability - level 3	Vuln
157889	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2019-4315)	Vulnerability - level 5	Vuln
157953	Oracle Enterprise Linux Security Update for python (ELSA-2019-0710)	Vulnerability - level 3	Vuln
157987	Oracle Enterprise Linux Security Update for curl (ELSA-2019-4652)	Vulnerability - level 4	Vuln
157999	Oracle Enterprise Linux Security Update for python (ELSA-2019-1467)	Vulnerability - level 3	Vuln
158042	Oracle Enterprise Linux Security Update for curl (ELSA-2019-1880)	Vulnerability - level 5	Vuln
158047	Oracle Enterprise Linux Security Update for python27:2.7 (ELSA-2019-0981)	Vulnerability - level 4	Vuln
158053	Oracle Enterprise Linux Security Update for python3 (ELSA-2019-0997)	Vulnerability - level 3	Vuln
158066	Oracle Enterprise Linux Security Update for pki-deps:10.6 (ELSA-2019-1529)	Vulnerability - level 4	Vuln
158085	Oracle Enterprise Linux Security Update for nss and nspr (ELSA-2019-1951)	Vulnerability - level 3	Vuln
158092	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2019-2471)	Vulnerability - level 3	Vuln
158101	Oracle Enterprise Linux Security Update for subversion:1.10 (ELSA-2019-2512)	Vulnerability - level 3	Vuln
158185	Oracle Enterprise Linux Security Update for nss (ELSA-2019-4114)	Vulnerability - level 3	Vuln
158188	Oracle Enterprise Linux Security Update for nss-softokn (ELSA-2019-4152)	Vulnerability - level 3	Vuln
158191	Oracle Enterprise Linux Security Update for nss, nss-softokn, nss-util (ELSA-2019-4190)	Vulnerability - level 3	Vuln
158285	Oracle Enterprise Linux Security Update for libvncserver (ELSA-2020-0920)	Vulnerability - level 3	Vuln
158286	Oracle Enterprise Linux Security Update for libvncserver (ELSA-2020-0913)	Vulnerability - level 3	Vuln
158441	Oracle Enterprise Linux Security Update for curl (ELSA-2019-2181)	Vulnerability - level 3	Vuln
158445	Oracle Enterprise Linux Security Update for tomcat (ELSA-2019-2205)	Vulnerability - level 4	Vuln
158447	Oracle Enterprise Linux Security Update for nss, nss-softokn, nss-util, and nspr (ELSA-2019-2237)	Vulnerability - level 3	Vuln
158538	Oracle Enterprise Linux Security Update for libreswan (ELSA-2020-2070)	Vulnerability - level 3	Vuln
158583	Oracle Enterprise Linux Security Update for sqlite (ELSA-2020-1810)	Vulnerability - level 4	Vuln
158586	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2020-1840)	Vulnerability - level 3	Vuln
158613	Oracle Enterprise Linux Security Update for microcode_ctl (ELSA-2020-2431)	Vulnerability - level 2	Vuln
158619	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5714)	Vulnerability - level 3	Vuln
158620	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5715)	Vulnerability - level 5	Vuln
158623	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5722)	Vulnerability - level 3	Vuln

158629	Oracle Enterprise Linux Security Update for microcode_ctl (ELSA-2020-2432)	Vulnerability - level 2	Vuln
158630	Oracle Enterprise Linux Security Update for microcode_ctl (ELSA-2020-2433)	Vulnerability - level 2	Vuln
158633	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5732)	Vulnerability - level 3	Vuln
158643	Oracle Enterprise Linux Security Update for nghttp2 (ELSA-2020-2755)	Vulnerability - level 3	Vuln
158661	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5750)	Vulnerability - level 3	Vuln
158664	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5755)	Vulnerability - level 4	Vuln
158665	Oracle Enterprise Linux Security Update for nodejs:10 (ELSA-2020-2848)	Vulnerability - level 3	Vuln
158666	Oracle Enterprise Linux Security Update for nodejs:12 (ELSA-2020-2852)	Vulnerability - level 3	Vuln
158673	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5756)	Vulnerability - level 3	Vuln
158694	Oracle Enterprise Linux Security Update for grub2 (ELSA-2020-5782)	Vulnerability - level 4	Vuln
158695	Oracle Enterprise Linux Security Update for grub2 (ELSA-2020-5786)	Vulnerability - level 4	Vuln
158696	Oracle Enterprise Linux Security Update for grub2 (ELSA-2020-5790)	Vulnerability - level 4	Vuln
158706	Oracle Enterprise Linux Security Update for libvncserver (ELSA-2020-3281)	Vulnerability - level 4	Vuln
158712	Oracle Enterprise Linux Security Update for libvncserver (ELSA-2020-3385)	Vulnerability - level 4	Vuln
158775	Oracle Enterprise Linux Security Update for subversion (ELSA-2020-3972)	Vulnerability - level 3	Vuln
158781	Oracle Enterprise Linux Security Update for libxml2 (ELSA-2020-3996)	Vulnerability - level 3	Vuln
158811	Oracle Enterprise Linux Security Update for nodejs:12 (ELSA-2020-4272)	Vulnerability - level 4	Vuln
158829	Oracle Enterprise Linux Security Update for ipa (ELSA-2020-3936)	Vulnerability - level 3	Vuln
158838	Oracle Enterprise Linux Security Update for sqlite (ELSA-2020-4442)	Vulnerability - level 3	Vuln
158847	Oracle Enterprise Linux Security Update for libxml2 (ELSA-2020-4479)	Vulnerability - level 3	Vuln
158908	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5913)	Vulnerability - level 4	Vuln
158919	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5914)	Vulnerability - level 2	Vuln
158920	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5917)	Vulnerability - level 2	Vuln
158923	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5926)	Vulnerability - level 2	Vuln
158966	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5995)	Vulnerability - level 5	Vuln
158967	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2020-5996)	Vulnerability - level 3	Vuln
158969	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2020-5476)	Vulnerability - level 3	Vuln
158973	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2020-5566-1)	Vulnerability - level 3	Vuln
158985	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9002)	Vulnerability - level 4	Vuln
158987	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9006)	Vulnerability - level 3	Vuln

158988	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9007)	Vulnerability - level 3	Vuln
158991	Oracle Enterprise Linux Security Update for dnsmasq (ELSA-2021-0150)	Vulnerability - level 4	Vuln
159010	Oracle Enterprise Linux Security Update for kernel (ELSA-2021-0558)	Vulnerability - level 3	Vuln
159032	Oracle Enterprise Linux Security Update for nodejs:10 (ELSA-2021-0548)	Vulnerability - level 4	Vuln
159042	Oracle Enterprise Linux Security Update for bind (ELSA-2021-0670)	Vulnerability - level 3	Vuln
159043	Oracle Enterprise Linux Security Update for bind (ELSA-2021-0671)	Vulnerability - level 3	Vuln
159051	Oracle Enterprise Linux Security Update for microcode_ctl (ELSA-2020-5083)	Vulnerability - level 2	Vuln
159052	Oracle Enterprise Linux Security Update for microcode_ctl (ELSA-2020-5084)	Vulnerability - level 2	Vuln
159053	Oracle Enterprise Linux Security Update for microcode_ctl (ELSA-2020-5085)	Vulnerability - level 2	Vuln
159056	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container kata-image kata-runtime kata kubernetes kubernetes istio olcne (ELSA-2020-5765)	Vulnerability - level 4	Vuln
159059	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2020-5923)	Vulnerability - level 2	Vuln
159060	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2020-5924)	Vulnerability - level 2	Vuln
159061	Oracle Enterprise Linux Security Update for grub2 (ELSA-2021-9076)	Vulnerability - level 3	Vuln
159062	Oracle Enterprise Linux Security Update for grub2 (ELSA-2021-9077)	Vulnerability - level 3	Vuln
159087	Oracle Enterprise Linux Security Update for grub2 (ELSA-2021-0699)	Vulnerability - level 3	Vuln
159088	Oracle Enterprise Linux Security Update for grub2 (ELSA-2021-0696)	Vulnerability - level 3	Vuln
159092	Oracle Enterprise Linux Security Update for nodejs:12 (ELSA-2021-0734)	Vulnerability - level 3	Vuln
159093	Oracle Enterprise Linux Security Update for nodejs:10 (ELSA-2021-0735)	Vulnerability - level 3	Vuln
159095	Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2021-0744)	Vulnerability - level 3	Vuln
159112	Oracle Enterprise Linux Security Update for kernel (ELSA-2021-0856)	Vulnerability - level 3	Vuln
159118	Oracle Enterprise Linux Security Update for bind (ELSA-2021-9117)	Vulnerability - level 3	Vuln
159128	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2021-1024)	Vulnerability - level 3	Vuln
159134	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2021-9137)	Vulnerability - level 3	Vuln
159137	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2021-9150)	Vulnerability - level 3	Vuln
159138	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2021-9151)	Vulnerability - level 3	Vuln
159160	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2021-9121)	Vulnerability - level 3	Vuln
159169	Oracle Enterprise Linux Security Update for openldap (ELSA-2021-1389)	Vulnerability - level 3	Vuln
159171	Oracle Enterprise Linux Security Update for bind (ELSA-2021-1469)	Vulnerability - level 3	Vuln
159174	Oracle Enterprise Linux Security Update for bind (ELSA-2021-9213)	Vulnerability - level 3	Vuln

159196	Oracle Enterprise Linux Security Update for curl (ELSA-2021-1610)	Vulnerability - level 3	Vuln
159219	Oracle Enterprise Linux Security Update for libvncserver (ELSA-2021-1811)	Vulnerability - level 3	Vuln
159232	Oracle Enterprise Linux Security Update for bind (ELSA-2021-1989)	Vulnerability - level 3	Vuln
159257	Oracle Enterprise Linux Security Update for microcode_ctl (ELSA-2021-2305)	Vulnerability - level 3	Vuln
159265	Oracle Enterprise Linux Security Update for postgresql:9.6 (ELSA-2021-2360)	Vulnerability - level 3	Vuln
159266	Oracle Enterprise Linux Security Update for postgresql:10 (ELSA-2021-2361)	Vulnerability - level 3	Vuln
159268	Oracle Enterprise Linux Security Update for postgresql:12 (ELSA-2021-2372)	Vulnerability - level 3	Vuln
159269	Oracle Enterprise Linux Security Update for postgresql:13 (ELSA-2021-2375)	Vulnerability - level 3	Vuln
159275	Oracle Enterprise Linux Security Update for postgresql (ELSA-2021-2397)	Vulnerability - level 3	Vuln
159284	Oracle Enterprise Linux Security Update for microcode_ctl (ELSA-2021-2308)	Vulnerability - level 3	Vuln
159285	Oracle Enterprise Linux Security Update for libxml2 (ELSA-2021-2569)	Vulnerability - level 4	Vuln
159327	Oracle Enterprise Linux Security Update for microcode_ctl (ELSA-2021-3027)	Vulnerability - level 3	Vuln
159328	Oracle Enterprise Linux Security Update for microcode_ctl (ELSA-2021-3028)	Vulnerability - level 3	Vuln
159338	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9404)	Vulnerability - level 3	Vuln
159339	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9406)	Vulnerability - level 3	Vuln
159369	Oracle Enterprise Linux Security Update for rh-postgresql10-postgresql (ELSA-2021-9428)	Vulnerability - level 3	Vuln
159374	Oracle Enterprise Linux Security Update for bind (ELSA-2021-3325)	Vulnerability - level 3	Vuln
159398	Oracle Enterprise Linux Security Update for nodejs:12 (ELSA-2021-3623)	Vulnerability - level 4	Vuln
159399	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9452)	Vulnerability - level 3	Vuln
159400	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9453)	Vulnerability - level 3	Vuln
159403	Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9459)	Vulnerability - level 4	Vuln
159408	Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2021-3666)	Vulnerability - level 4	Vuln
159414	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2021-3798)	Vulnerability - level 3	Vuln
159418	Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2021-3816)	Vulnerability - level 4	Vuln
159423	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2021-9478)	Vulnerability - level 3	Vuln
159438	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2021-9528)	Vulnerability - level 3	Vuln
159492	Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)	Vulnerability - level 3	Vuln
159501	Oracle Enterprise Linux Security Update for bind (ELSA-2021-4384)	Vulnerability - level 3	Vuln
159506	Oracle Enterprise Linux Security Update for sqlite (ELSA-2021-4396)	Vulnerability - level 3	Vuln
159512	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2021-4424)	Vulnerability - level 3	Vuln

159535	Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4647)	Vulnerability - level 4	Vuln
159553	Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2021-5160)	Vulnerability - level 3	Vuln
159562	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2021-9561)	Vulnerability - level 3	Vuln
159570	Oracle Enterprise Linux Security Update for httpd (ELSA-2021-9619)	Vulnerability - level 4	Vuln
159574	Oracle Enterprise Linux Security Update for openssl (ELSA-2021-5226)	Vulnerability - level 3	Vuln
159581	Oracle Enterprise Linux Security Update for openssl (ELSA-2021-9632)	Vulnerability - level 3	Vuln
159585	Oracle Enterprise Linux Security Update for grafana (ELSA-2022-0001)	Vulnerability - level 3	Vuln
159589	Oracle Enterprise Linux Security Update for openssl (ELSA-2022-0064)	Vulnerability - level 3	Vuln
159594	Oracle Enterprise Linux Security Update for httpd (ELSA-2022-0143)	Vulnerability - level 4	Vuln
159609	Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-9005)	Vulnerability - level 4	Vuln
159615	Oracle Enterprise Linux Security Update for openssl (ELSA-2022-9017)	Vulnerability - level 3	Vuln
159616	Oracle Enterprise Linux Security Update for openssl (ELSA-2022-9023)	Vulnerability - level 3	Vuln
159622	Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2022-0350)	Vulnerability - level 4	Vuln
159648	Oracle Enterprise Linux Security Update for openldap (ELSA-2022-0621)	Vulnerability - level 4	Vuln
159652	Oracle Enterprise Linux Security Update for idm:dl1 and idm:client (ELSA-2020-4670)	Vulnerability - level 3	Vuln
159679	Oracle Enterprise Linux Security Update for pki-core:10.6 and pki-deps:10.6 (ELSA-2020-4847)	Vulnerability - level 3	Vuln
159681	Oracle Enterprise Linux Security Update for subversion:1.10 (ELSA-2020-4712)	Vulnerability - level 3	Vuln
159696	Oracle Enterprise Linux Security Update for firefox (ELSA-2022-0824)	Vulnerability - level 5	Vuln
159697	Oracle Enterprise Linux Security Update for firefox (ELSA-2022-0818)	Vulnerability - level 5	Vuln
159705	Oracle Enterprise Linux Security Update for thunderbird (ELSA-2022-0845)	Vulnerability - level 5	Vuln
159706	Oracle Enterprise Linux Security Update for thunderbird (ELSA-2022-0850)	Vulnerability - level 5	Vuln
159707	Oracle Enterprise Linux Security Update for libxml2 (ELSA-2022-0899)	Vulnerability - level 4	Vuln
159711	Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-0891)	Vulnerability - level 5	Vuln
159712	Oracle Enterprise Linux Security Update for expat (ELSA-2022-0951)	Vulnerability - level 5	Vuln
159714	Oracle Enterprise Linux Security Update for expat (ELSA-2022-9227)	Vulnerability - level 5	Vuln
159719	Oracle Enterprise Linux Security Update for expat (ELSA-2022-9232)	Vulnerability - level 5	Vuln
159727	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9245)	Vulnerability - level 4	Vuln
159729	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9244)	Vulnerability - level 4	Vuln
159731	Oracle Enterprise Linux Security Update for httpd (ELSA-2022-1045)	Vulnerability - level 5	Vuln

159732	Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-1049)	Vulnerability - level 5	Vuln
159733	Oracle Enterprise Linux Security Update for expat (ELSA-2022-1069)	Vulnerability - level 5	Vuln
159739	Oracle Enterprise Linux Security Update for httpd (ELSA-2022-9257)	Vulnerability - level 5	Vuln
159754	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9274)	Vulnerability - level 4	Vuln
159755	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9273)	Vulnerability - level 4	Vuln
159760	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9314)	Vulnerability - level 4	Vuln
159763	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9313)	Vulnerability - level 4	Vuln
159776	Oracle Enterprise Linux Security Update for xmlrpc-c (ELSA-2022-1643)	Vulnerability - level 5	Vuln
159782	Oracle Enterprise Linux Security Update for expat (ELSA-2022-9359)	Vulnerability - level 4	Vuln
159783	Oracle Enterprise Linux Security Update for olcne istio istio (ELSA-2022-9362)	Vulnerability - level 4	Vuln
159784	Oracle Enterprise Linux Security Update for olcne istio istio (ELSA-2022-9363)	Vulnerability - level 4	Vuln
159810	Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2022-1819)	Vulnerability - level 5	Vuln
159815	Oracle Enterprise Linux Security Update for bind (ELSA-2022-2092)	Vulnerability - level 3	Vuln
159825	Oracle Enterprise Linux Security Update for kernel (ELSA-2022-1988)	Vulnerability - level 5	Vuln
159848	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9410)	Vulnerability - level 4	Vuln
159849	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9412)	Vulnerability - level 4	Vuln
159850	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9413)	Vulnerability - level 4	Vuln
159852	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9409)	Vulnerability - level 4	Vuln
159885	Oracle Enterprise Linux Security Update for go-toolset:ol8addon (ELSA-2022-14844)	Vulnerability - level 4	Vuln
159886	Oracle Enterprise Linux Security Update for go-toolset:ol8addon (ELSA-2022-14857)	Vulnerability - level 5	Vuln
159890	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9477)	Vulnerability - level 4	Vuln
159895	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9478)	Vulnerability - level 4	Vuln
159896	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9479)	Vulnerability - level 4	Vuln
159899	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9480)	Vulnerability - level 4	Vuln
159915	Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5232)	Vulnerability - level 4	Vuln
159918	Oracle Enterprise Linux Security Update for expat (ELSA-2022-5314)	Vulnerability - level 4	Vuln
159925	Oracle Enterprise Linux Security Update for expat (ELSA-2022-5244)	Vulnerability - level 4	Vuln
159931	Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5249)	Vulnerability - level 4	Vuln
159959	Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2022-5337)	Vulnerability - level 4	Vuln

159969	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9557)	Vulnerability - level 4	Vuln
159981	Oracle Enterprise Linux Security Update for go-toolset:ol8addon (ELSA-2022-17956)	Vulnerability - level 4	Vuln
159984	Oracle Enterprise Linux Security Update for ol8addon (ELSA-2022-17957)	Vulnerability - level 4	Vuln
159987	Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5564)	Vulnerability - level 4	Vuln
160014	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2022-5818)	Vulnerability - level 5	Vuln
160015	Oracle Enterprise Linux Security Update for httpd (ELSA-2022-9676)	Vulnerability - level 5	Vuln
160016	Oracle Enterprise Linux Security Update for httpd (ELSA-2022-9675)	Vulnerability - level 5	Vuln
160022	Oracle Enterprise Linux Security Update for httpd (ELSA-2022-9680)	Vulnerability - level 5	Vuln
160025	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2022-9683)	Vulnerability - level 5	Vuln
160040	Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-9682)	Vulnerability - level 5	Vuln
160072	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2022-6224)	Vulnerability - level 5	Vuln
160092	Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2022-6448)	Vulnerability - level 5	Vuln
160094	Oracle Enterprise Linux Security Update for nodejs:16 (ELSA-2022-6449)	Vulnerability - level 5	Vuln
160111	Oracle Enterprise Linux Security Update for nodejs and nodejs-nodemon (ELSA-2022-6595)	Vulnerability - level 5	Vuln
160123	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9852)	Vulnerability - level 4	Vuln
160171	Oracle Enterprise Linux Security Update for kernel (ELSA-2022-7110)	Vulnerability - level 4	Vuln
160196	Oracle Enterprise Linux Security Update for pcs (ELSA-2022-7343)	Vulnerability - level 3	Vuln
160207	Oracle Enterprise Linux Security Update for bind (ELSA-2022-7790)	Vulnerability - level 4	Vuln
160210	Oracle Enterprise Linux Security Update for kernel (ELSA-2022-7683)	Vulnerability - level 4	Vuln
160219	Oracle Enterprise Linux Security Update for bind9.16 (ELSA-2022-7643)	Vulnerability - level 4	Vuln
160232	Oracle Enterprise Linux Security Update for xmlrpc-c (ELSA-2022-7692)	Vulnerability - level 5	Vuln
160233	Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2022-7457)	Vulnerability - level 4	Vuln
160243	Oracle Enterprise Linux Security Update for e2fsprogs (ELSA-2022-7720)	Vulnerability - level 4	Vuln
160250	Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-7647)	Vulnerability - level 5	Vuln
160270	Oracle Enterprise Linux Security Update for kernel (ELSA-2022-8267)	Vulnerability - level 4	Vuln
160283	Oracle Enterprise Linux Security Update for e2fsprogs (ELSA-2022-8361)	Vulnerability - level 4	Vuln
160287	Oracle Enterprise Linux Security Update for dhcp security and enhancement update (ELSA-2022-8385)	Vulnerability - level 4	Vuln
160309	Oracle Enterprise Linux Security Update for httpd (ELSA-2022-8067)	Vulnerability - level 5	Vuln
160313	Oracle Enterprise Linux Security Update for bind (ELSA-2022-8068)	Vulnerability - level 4	Vuln
160346	Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-26385)	Vulnerability - level 4	Vuln

160426	Oracle Enterprise Linux Security Update for bind (ELSA-2023-0402)	Vulnerability - level 4	Vuln
160429	Oracle Enterprise Linux Security Update for kernel (ELSA-2023-0399)	Vulnerability - level 4	Vuln
160481	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-0946)	Vulnerability - level 4	Vuln
160492	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-12152)	Vulnerability - level 4	Vuln
160512	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-1335)	Vulnerability - level 4	Vuln
160517	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-12205)	Vulnerability - level 4	Vuln
160519	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-12210)	Vulnerability - level 4	Vuln
160521	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-1405)	Vulnerability - level 4	Vuln
160523	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-12213)	Vulnerability - level 4	Vuln
160563	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-12297)	Vulnerability - level 4	Vuln
160576	Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-12326)	Vulnerability - level 4	Vuln
160621	Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-2165)	Vulnerability - level 5	Vuln
160668	Oracle Enterprise Linux Security Update for edk2 (ELSA-2023-2932)	Vulnerability - level 4	Vuln
165002	SUSE Security Update for krb5 (SUSE-SA:2009:019)	Vulnerability - level 3	Vuln
165009	SUSE Security Update for Sun Java (SUSE-SA:2009:001)	Vulnerability - level 3	Vuln
165021	SUSE Security Update for Mozilla Firefox (SUSE-SA:2008:034)	Vulnerability - level 3	Vuln
165028	SUSE Security Update for Kernel (SUSE-SA:2008:030)	Vulnerability - level 3	Vuln
165040	SUSE Security Update for Samba (SUSE-SA:2007:065)	Vulnerability - level 3	Vuln
165044	SUSE Security Update for Flash Player (SUSE-SA:2007:069)	Vulnerability - level 3	Vuln
165047	SUSE Security Update for Apache2 (SUSE-SA:2007:061)	Vulnerability - level 3	Vuln
165075	OpenSUSE Security Update for Samba (SUSE-SA:2007:031)	Vulnerability - level 3	Vuln
165089	SUSE Security Update for Samba (SUSE-SA:2007:016)	Vulnerability - level 3	Vuln
165122	SUSE Security Update for Opera (SUSE-SA:2006:061)	Vulnerability - level 3	Vuln
165127	SUSE Security Update for php4, php5 (SUSE-SA:2006:052)	Vulnerability - level 3	Vuln
165153	SUSE Security Update for cyrus-sasl-digestmd5 (SUSE-SA:2006:025)	Vulnerability - level 3	Vuln
165156	SUSE Update for Multiple Packages (SUSE-SR:2010:004)	Vulnerability - level 3	Vuln
165161	SUSE Security Update for Kernel (SUSE-SA:2010:054)	Vulnerability - level 4	Vuln
165165	SUSE Security Update for Multiple Packages (SUSE-SR:2010:022)	Vulnerability - level 4	Vuln
165166	SUSE Security Update for Multiple Packages (SUSE-SR:2010:017)	Vulnerability - level 4	Vuln
165167	SUSE Security Update for Multiple Packages (SUSE-SR:2010:023)	Vulnerability - level 4	Vuln
165170	SUSE Security Update for Kernel (SUSE-SA:2011:001)	Vulnerability - level 4	Vuln
165171	SUSE Security Update for kernel (SUSE-SA:2011:002)	Vulnerability - level 4	Vuln
165173	SUSE Security Update for Multiple Packages (SUSE-SR:2011:001)	Vulnerability - level 5	Vuln
165174	SUSE Security Update for Multiple Packages (SUSE-SR:2011:002)	Vulnerability - level 5	Vuln
165180	SUSE Security Update for Kernel (SUSE-SA:2011:017)	Vulnerability - level 4	Vuln
165182	SUSE Security Update for Kernel (SUSE-SA:2011:020)	Vulnerability - level 5	Vuln
165183	SUSE Security Update for Kernel (SUSE-SA:2011:021)	Vulnerability - level 5	Vuln
165186	SUSE Security Update for Multiple Packages (SUSE-SR:2011:004)	Vulnerability - level 4	Vuln
165187	SUSE Security Update for Multiple Packages (SUSE-SR:2011:005)	Vulnerability - level 5	Vuln
165190	SUSE Security Update for Multiple Packages (SUSE-SR:2011:008)	Vulnerability - level 5	Vuln
165191	SUSE Security Update for Multiple Packages (SUSE-SR:2011:009)	Vulnerability - level 5	Vuln
165193	SUSE Security Update for Postfix (SUSE-SA:2011:023)	Vulnerability - level 3	Vuln
165195	SUSE Security Update for Multiple Packages (SUSE-SR:2011:010)	Vulnerability - level 4	Vuln
165197	SUSE Security Update for Multiple Packages (SUSE-SR:2010:018)	Vulnerability - level 5	Vuln
165198	SUSE Security Update for Multiple Packages (SUSE-SR:2010:019)	Vulnerability - level 5	Vuln

165205	SUSE Security Update for Kernel (SUSE-SA:2010:039)	Vulnerability - level 4	Vuln
165206	SUSE Security Update for Kernel (SUSE-SA:2010:041)	Vulnerability - level 4	Vuln
165210	SUSE Security Update for Multiple Packages (SUSE-SR:2010:017) - Deprecated	Vulnerability - level 4	Vuln
165212	SUSE Security Update for Multiple Packages (SUSE-SR:2010:014)	Vulnerability - level 5	Vuln
165213	SUSE Security Update for Multiple Packages (SUSE-SR:2010:015)	Vulnerability - level 5	Vuln
165214	SUSE Security Update for Multiple Packages (SUSE-SR:2010:016)	Vulnerability - level 5	Vuln
165218	SUSE Security Update for Kernel (SUSE-SA:2010:031)	Vulnerability - level 4	Vuln
165221	SUSE Security Update for Multiple Packages (SUSE-SR:2010:013)	Vulnerability - level 5	Vuln
165222	SUSE Security Update for Multiple Packages (SUSE-SR:2010:011)	Vulnerability - level 5	Vuln
165223	SUSE Security Update for Multiple Packages (SUSE-SR:2010:012)	Vulnerability - level 4	Vuln
165224	SUSE Security Update for OpenSSL (SUSE-SA:2010:020)	Vulnerability - level 5	Vuln
165225	SUSE Security Update for Multiple Packages (SUSE-SR:2010:008)	Vulnerability - level 5	Vuln
165226	SUSE Security Update for Multiple Packages (SUSE-SR:2010:009)	Vulnerability - level 5	Vuln
165227	SUSE Security Update for Multiple Packages (SUSE-SA:2010:021)	Vulnerability - level 5	Vuln
165230	SUSE Security Update for Kernel (SUSE-SA:2010:014)	Vulnerability - level 5	Vuln
165231	SUSE Security Update for Mozilla, Firefox, SeaMonkey (SUSE-SA:2010:015)	Vulnerability - level 5	Vuln
165232	SUSE Security Update for Kernel (SUSE-SA:2010:016)	Vulnerability - level 4	Vuln
165234	SUSE Security Update for OpenOffice_org (SUSE-SA:2010:017)	Vulnerability - level 5	Vuln
165235	SUSE Security Update for Kernel (SUSE-SA:2010:018)	Vulnerability - level 4	Vuln
165238	SUSE Security Update for Kernel (SUSE-SA:2010:010)	Vulnerability - level 5	Vuln
165239	SUSE Security Update for Multiple Packages (SUSE-SR:2010:003)	Vulnerability - level 5	Vuln
165241	SUSE Security Update for Kernel (SUSE-SA:2010:012)	Vulnerability - level 5	Vuln
165242	SUSE Security Update for Multiple Packages (SUSE-SR:2010:004)	Vulnerability - level 5	Vuln
165243	SUSE Security Update for Multiple Packages (SUSE-SR:2010:005)	Vulnerability - level 4	Vuln
165244	SUSE Security Update for Kernel (SUSE-SA:2010:001)	Vulnerability - level 4	Vuln
165246	SUSE Security Update for Kernel (SUSE-SA:2010:005)	Vulnerability - level 5	Vuln
165247	SUSE Security Update for krb5 (SUSE-SA:2010:006)	Vulnerability - level 5	Vuln
165262	SUSE Security Update for compat-openssl097g (openSUSE-SU-2011:0845-1)	Vulnerability - level 3	Vuln
165266	SUSE Security Update for krb5-appl (openSUSE-SU-2012:0019-1)	Vulnerability - level 5	Vuln
165269	SUSE Security Update for krb5-appl (openSUSE-SU-2012:0051-1)	Vulnerability - level 5	Vuln
165276	SUSE Security Update for kernel (openSUSE-SU-2012:0206-1)	Vulnerability - level 3	Vuln
165384	SUSE Security Update for java-1_6_0-openjdk: icedtea-web update to 1.11.4 (openSUSE-SU-2012:1175-1)	Vulnerability - level 5	Vuln
165387	SUSE Security Update for freeradius: Fix Stack Overflow in TLS Handling (openSUSE-SU-2012:1200-1)	Vulnerability - level 3	Vuln
165390	SUSE Security Update for rubygem-actionpack-2_3, rubygem-activesupport-2_3 (openSUSE-SU-2012:1218-1)	Vulnerability - level 2	Vuln
165396	SUSE Security Update for libproxy, libproxy-plugins (openSUSE-SU-2012:1375-1)	Vulnerability - level 3	Vuln
165411	SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2012:1488-1)	Vulnerability - level 2	Vuln
165420	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2012:1391-1)	Vulnerability - level 4	Vuln
165421	SUSE Enterprise Linux Security Update for rubygem-actionpack-2_3 (SUSE-SU-2012:1367-1)	Vulnerability - level 3	Vuln
165426	SUSE Enterprise Linux Security Update for IBM Java (SUSE-SU-2012:1265-1)	Vulnerability - level 4	Vuln
165427	SUSE Enterprise Linux Security Update for IBM Java (SUSE-SU-2012:1231-1)	Vulnerability - level 4	Vuln
165433	SUSE Enterprise Linux Security Update for Mozilla Firefox (SUSE-SU-2012:1167-1)	Vulnerability - level 5	Vuln
165435	SUSE Enterprise Linux Security Update for Mozilla Firefox (SUSE-SU-2012:1157-1)	Vulnerability - level 5	Vuln
165441	SUSE Enterprise Linux Security Update for OpenJDK (SUSE-SU-2012:1148-1)	Vulnerability - level 5	Vuln
165474	SUSE Enterprise Linux Update for Kernel (SUSE-SU-2012:0689-1)	Vulnerability - level 4	Vuln

165479	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2012:0736-1)	Vulnerability - level 4	Vuln
165480	SUSE Enterprise Linux Security Update for t1lib (SUSE-SU-2012:0740-1)	Vulnerability - level 3	Vuln
165487	SUSE Enterprise Linux Security Update for t1lib (SUSE-SU-2012:0744-1)	Vulnerability - level 3	Vuln
165492	SUSE Enterprise Linux Security Update for dhcpcd (SUSE-SU-2012:0767-1)	Vulnerability - level 3	Vuln
165522	SUSE Enterprise Linux Security Update for libxslt (SUSE-SU-2012:0901-1)	Vulnerability - level 2	Vuln
165523	SUSE Enterprise Linux Security Update for libexif (SUSE-SU-2012:0902-1)	Vulnerability - level 4	Vuln
165524	SUSE Enterprise Linux Security Update for libexif (SUSE-SU-2012:0903-1)	Vulnerability - level 4	Vuln
165525	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2012:0904-1)	Vulnerability - level 3	Vuln
165526	SUSE Enterprise Linux Security Update for libtiff (SUSE-SU-2012:0919-1)	Vulnerability - level 3	Vuln
165548	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:004)	Vulnerability - level 3	Vuln
165549	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:005)	Vulnerability - level 3	Vuln
165550	SUSE Enterprise Linux Security Update IBM Java 6 (SUSE-SA:2011:006)	Vulnerability - level 3	Vuln
165551	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:008)	Vulnerability - level 3	Vuln
165554	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:012)	Vulnerability - level 3	Vuln
165555	SUSE Enterprise Linux Security Update IBM Java (SUSE-SA:2011:014)	Vulnerability - level 3	Vuln
165558	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:019)	Vulnerability - level 3	Vuln
165562	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:026)	Vulnerability - level 3	Vuln
165563	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:027)	Vulnerability - level 3	Vuln
165567	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:031)	Vulnerability - level 3	Vuln
165570	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:034)	Vulnerability - level 3	Vuln
165577	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:042)	Vulnerability - level 3	Vuln
165581	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2011:046)	Vulnerability - level 3	Vuln
165583	SUSE Enterprise Linux Security Update krb5 (SUSE-SA:2010:006)	Vulnerability - level 3	Vuln
165584	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:007)	Vulnerability - level 3	Vuln
165586	SUSE Enterprise Linux Security Update Mozilla Firefox (SUSE-SA:2010:015)	Vulnerability - level 3	Vuln
165587	SUSE Enterprise Linux Security Update OpenOffice.org (SUSE-SA:2010:017)	Vulnerability - level 3	Vuln
165588	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:019)	Vulnerability - level 3	Vuln
165589	SUSE Enterprise Linux Security Update Mozilla Firefox 3.5.9 (SUSE-SA:2010:021)	Vulnerability - level 3	Vuln
165591	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:023)	Vulnerability - level 3	Vuln
165594	SUSE Enterprise Linux Security Update IBM Java 6 (SUSE-SA:2010:026)	Vulnerability - level 3	Vuln

165596	SUSE Enterprise Linux Security Update IBM Java 5 (SUSE-SA:2010:028)	Vulnerability - level 3	Vuln
165599	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:031)	Vulnerability - level 3	Vuln
165601	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:033)	Vulnerability - level 3	Vuln
165603	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:035)	Vulnerability - level 3	Vuln
165605	SUSE Enterprise Linux Security Update Kernel (SUSE-SA:2010:038)	Vulnerability - level 3	Vuln
165606	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:040)	Vulnerability - level 3	Vuln
165607	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:041)	Vulnerability - level 3	Vuln
165610	SUSE Enterprise Linux Security Update SUSE Linux Enterprise 10 SP3 Kernel (SUSE-SA:2010:044)	Vulnerability - level 3	Vuln
165614	SUSE Enterprise Linux Security Update For Multiple Applications	Vulnerability - level 3	Vuln
165615	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:050)	Vulnerability - level 3	Vuln
165617	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:054)	Vulnerability - level 3	Vuln
165620	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2010:057)	Vulnerability - level 3	Vuln
165622	SUSE Enterprise Linux Security Update Linux kernel (SUSE-SA:2010:060)	Vulnerability - level 3	Vuln
165623	SUSE Enterprise Linux Security Update IBM Java 1.4.2 (SUSE-SA:2010:061)	Vulnerability - level 3	Vuln
165624	SUSE Enterprise Linux Security Update Sun Java (SUSE-SA:2009:001)	Vulnerability - level 3	Vuln
165628	SUSE Enterprise Linux Security Update IBM Java 5 (SUSE-SA:2009:007)	Vulnerability - level 3	Vuln
165632	SUSE Enterprise Linux Security Update (SUSE-SR:2009:012)	Vulnerability - level 3	Vuln
165636	SUSE Enterprise Linux Security Update IBM Java 1.4.2 and 6 (SUSE-SA:2009:018)	Vulnerability - level 3	Vuln
165637	SUSE Enterprise Linux Security Update krb5 (SUSE-SA:2009:019)	Vulnerability - level 3	Vuln
165638	SUSE Enterprise Linux Security Update (SUSE-SR:2009:001)	Vulnerability - level 3	Vuln
165646	SUSE Enterprise Linux Security Update (SUSE-SR:2009:002)	Vulnerability - level 3	Vuln
165648	SUSE Enterprise Linux Security Update Acrobat Reader (SUSE-SA:2009:035)	Vulnerability - level 3	Vuln
165653	SUSE Enterprise Linux Security Update Subversion (SUSE-SA:2009:044)	Vulnerability - level 3	Vuln
165659	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2009:051)	Vulnerability - level 3	Vuln
165661	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2009:054)	Vulnerability - level 3	Vuln
165663	SUSE Enterprise Linux Security Update BIND (SUSE-SA:2009:059)	Vulnerability - level 3	Vuln
165675	SUSE Enterprise Linux Security Update krb5 (SUSE-SA:2008:016)	Vulnerability - level 3	Vuln
165680	SUSE Enterprise Linux Security Update Apache,Apache2 Security Problems (SUSE-SA:2008:021)	Vulnerability - level 3	Vuln
165684	SUSE Enterprise Linux Security Update (SUSE-SR:2008:023)	Vulnerability - level 3	Vuln
165690	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2008:032)	Vulnerability - level 2	Vuln
165692	SUSE Enterprise Linux Security Update Mozilla Firefox (SUSE-SA:2008:034)	Vulnerability - level 3	Vuln
165693	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2008:035)	Vulnerability - level 3	Vuln
165694	SUSE Enterprise Linux Security Update Linux Kernel (SUSE-SA:2008:038)	Vulnerability - level 3	Vuln
165709	SUSE Enterprise Linux Security Update (SUSE-SR:2008:005)	Vulnerability - level 3	Vuln
165710	SUSE Enterprise Linux Security Update (SUSE-SR:2008:008)	Vulnerability - level 4	Vuln

165729	SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2012:1666-1)	Vulnerability - level 3	Vuln
165737	SUSE Enterprise Linux Security Update for rubygem-actionpack-2_3 (SUSE-SU-2013:0208-1)	Vulnerability - level 3	Vuln
165738	SUSE Enterprise Linux Security Update for tomcat6 (SUSE-SU-2013:0226-1)	Vulnerability - level 3	Vuln
165739	SUSE Enterprise Linux Security Update for tomcat5 (SUSE-SU-2013:0228-1)	Vulnerability - level 3	Vuln
165745	SUSE Enterprise Linux Security Update for Samba (SUSE-SU-2013:0325-1)	Vulnerability - level 4	Vuln
165746	SUSE Enterprise Linux Security Update for Samba (SUSE-SU-2013:0326-1)	Vulnerability - level 4	Vuln
165747	SUSE Enterprise Linux Security Update for Java (SUSE-SU-2013:0328-1)	Vulnerability - level 4	Vuln
165765	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2013:0469-1)	Vulnerability - level 4	Vuln
165766	SUSE Enterprise Linux Security Update for Mozilla Firefox (SUSE-SU-2013:0470-1)	Vulnerability - level 4	Vuln
165767	SUSE Enterprise Linux Security Update for Mozilla Firefox (SUSE-SU-2013:0471-1)	Vulnerability - level 4	Vuln
165769	SUSE Enterprise Linux Security Update for Samba (SUSE-SU-2013:0519-1)	Vulnerability - level 4	Vuln
165771	SUSE Enterprise Linux Security Update for OpenSSL (SUSE-SU-2013:0549-1)	Vulnerability - level 3	Vuln
165772	SUSE Enterprise Linux Security Update for OpenSSL (SUSE-SU-2013:0554-1)	Vulnerability - level 3	Vuln
165777	SUSE Enterprise Linux Security Update for PostgreSQL (SUSE-SU-2013:0633-1)	Vulnerability - level 4	Vuln
165779	SUSE Enterprise Linux Security Update for Apache (SUSE-SU-2013:0648-1)	Vulnerability - level 3	Vuln
165780	SUSE Enterprise Linux Security Update for flash-player (SUSE-SU-2013:0670-1)	Vulnerability - level 4	Vuln
165781	SUSE Enterprise Linux Security Update for flash-player (SUSE-SU-2013:0670-2)	Vulnerability - level 4	Vuln
165782	SUSE Enterprise Linux Security Update for OpenSSL (SUSE-SU-2013:0549-3)	Vulnerability - level 3	Vuln
165783	SUSE Enterprise Linux Security Update for PostgreSQL (SUSE-SU-2013:0633-2)	Vulnerability - level 4	Vuln
165785	SUSE Enterprise Linux Security Update for Ruby on Rails (SUSE-SU-2013:0707-1)	Vulnerability - level 3	Vuln
165788	SUSE Enterprise Linux Security Update for dhcp (SUSE-SU-2013:0696-1)	Vulnerability - level 3	Vuln
165789	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2013:0743-1)	Vulnerability - level 3	Vuln
165790	SUSE Enterprise Linux Security Update for Linux kernel (SUSE-SU-2013:0759-1)	Vulnerability - level 4	Vuln
165795	SUSE Enterprise Linux Security Update for libtiff (SUSE-SU-2013:0795-1)	Vulnerability - level 3	Vuln
165800	SUSE Security Update for java-1_7_0-openjdk (openSUSE-SU-2013:0745-1)	Vulnerability - level 5	Vuln
165801	SUSE Security Update for Strongswan (openSUSE-SU-2013:0774-1)	Vulnerability - level 2	Vuln
165802	SUSE Security Update for Strongswan (openSUSE-SU-2013:0775-1)	Vulnerability - level 2	Vuln
165803	SUSE Security Update for xorg-x11-server (openSUSE-SU-2013:0776-1)	Vulnerability - level 1	Vuln
165804	SUSE Security Update for java-1_6_0-openjdk to Icedtea6-1.12.5 (openSUSE-SU-2013:0777-1)	Vulnerability - level 5	Vuln
165808	SUSE Security Update for tiff (openSUSE-SU-2013:0812-1)	Vulnerability - level 3	Vuln
165809	SUSE Security Update for tiff (openSUSE-SU-2013:0812-2)	Vulnerability - level 3	Vuln
165831	SUSE Security Update for tomcat6 (openSUSE-SU-2013:0147-1)	Vulnerability - level 3	Vuln

165840	SUSE Security Update for tomcat6 (openSUSE-SU-2013:0161-1)	Vulnerability - level 2	Vuln
165852	SUSE Security Update for libtcnative-1-0 and tomcat6 (openSUSE-SU-2013:0192-1)	Vulnerability - level 2	Vuln
165860	SUSE Security Update for java-1_6_0-openjdk (openSUSE-SU-2013:0375-1)	Vulnerability - level 5	Vuln
165863	SUSE Security Update for java-1_6_0-openjdk (openSUSE-SU-2013:0378-1)	Vulnerability - level 5	Vuln
165875	SUSE Security Update for Mozilla (openSUSE-SU-2013:0431-1)	Vulnerability - level 5	Vuln
165881	SUSE Security Update for MozillaThunderbird (openSUSE-SU-2013:0465-1)	Vulnerability - level 5	Vuln
165882	SUSE Security Update for xulrunner (openSUSE-SU-2013:0466-1)	Vulnerability - level 5	Vuln
165883	SUSE Security Update for MozillaFirefox (openSUSE-SU-2013:0467-1)	Vulnerability - level 5	Vuln
165884	SUSE Security Update for Seamonkey (openSUSE-SU-2013:0468-1)	Vulnerability - level 5	Vuln
165897	SUSE Security Update for nss-pam-ldapd (openSUSE-SU-2013:0522-1)	Vulnerability - level 3	Vuln
165898	SUSE Security Update for nss-pam-ldapd (openSUSE-SU-2013:0522-2)	Vulnerability - level 3	Vuln
165899	SUSE Security Update for nss-pam-ldapd (openSUSE-SU-2013:0524-1)	Vulnerability - level 3	Vuln
165902	SUSE Security Update for sssd (openSUSE-SU-2013:0559-1)	Vulnerability - level 2	Vuln
165906	SUSE Enterprise Linux Security Update for Apache (SUSE-SU-2013:0648-2)	Vulnerability - level 3	Vuln
165907	SUSE Enterprise Linux Security Update for Apache (SUSE-SU-2013:0830-1)	Vulnerability - level 3	Vuln
165908	SUSE Enterprise Linux Security Update for IBM Java (SUSE-SU-2013:0835-1)	Vulnerability - level 4	Vuln
165912	SUSE Enterprise Linux Security Update for Subversion (SUSE-SU-2013:0838-1)	Vulnerability - level 3	Vuln
165914	SUSE Security Update for Kernel (openSUSE-SU-2013:0824-1)	Vulnerability - level 4	Vuln
165919	SUSE Security Update for Kernel (openSUSE-SU-2013:0847-1)	Vulnerability - level 4	Vuln
165922	SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2013:0857-1)	Vulnerability - level 2	Vuln
165923	SUSE Enterprise Linux Security update for Xorg(SUSE-SU-2013:0859-1)	Vulnerability - level 2	Vuln
165947	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2013:1182-2)	Vulnerability - level 4	Vuln
165951	SUSE Enterprise Linux Security Update for Subversion (SUSE-SU-2013:1217-1)	Vulnerability - level 3	Vuln
165953	SUSE Enterprise Linux Security Update for Strongswan (SUSE-SU-2013:1237-1)	Vulnerability - level 3	Vuln
165963	SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2013:1237-2)	Vulnerability - level 3	Vuln
165964	SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2013:1237-3)	Vulnerability - level 3	Vuln
165966	SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2013:1251-1)	Vulnerability - level 3	Vuln
165968	SUSE Enterprise Linux Security Update for ruby (SUSE-SU-2013:1260-2)	Vulnerability - level 3	Vuln
165969	SUSE Enterprise Linux Security Update for Ruby (SUSE-SU-2013:1260-3)	Vulnerability - level 3	Vuln
165971	SUSE Enterprise Linux Security Update for PHP5 (SUSE-SU-2013:1285-1)	Vulnerability - level 4	Vuln
165982	SUSE Enterprise Linux Security Update for krb5 (SUSE-SU-2013:1190-1)	Vulnerability - level 3	Vuln
165984	SUSE Security Update for Strongswan (openSUSE-SU-2013:0873-1)	Vulnerability - level 2	Vuln
165987	SUSE Security Update for xorg-x11-server (openSUSE-SU-2013:0878-1)	Vulnerability - level 1	Vuln
165999	SUSE Security Update for tiff (openSUSE-SU-2013:0922-1)	Vulnerability - level 5	Vuln

166000	SUSE Security Update for Kerne (openSUSE-SU-2013:0923-1)	Vulnerability - level 4	Vuln
166001	SUSE Security Update for Kernel (openSUSE-SU-2013:0925-1)	Vulnerability - level 4	Vuln
166002	SUSE Security Update for Update Kernel to 3.0 (openSUSE-SU-2013:0927-1)	Vulnerability - level 4	Vuln
166005	SUSE Security Update for xorg-x11-server (openSUSE-SU-2013:0937-1)	Vulnerability - level 1	Vuln
166008	SUSE Security Update for tiff (openSUSE-SU-2013:0944-1)	Vulnerability - level 5	Vuln
166015	SUSE Security Update for java-1_7_0-openjdk (openSUSE-SU-2013:0964-1)	Vulnerability - level 5	Vuln
166018	SUSE Security Update for Strongswan (openSUSE-SU-2013:0985-1)	Vulnerability - level 2	Vuln
166020	SUSE Security Update for java-1_6_0-openjdk (openSUSE-SU-2013:0993-1)	Vulnerability - level 5	Vuln
166022	SUSE Security Update for Subversion (openSUSE-SU-2013:1006-1)	Vulnerability - level 4	Vuln
166029	SUSE Security Update for telepathy-gabble (openSUSE-SU-2013:1013-1)	Vulnerability - level 3	Vuln
166058	SUSE Security Update for openstack-keystone (openSUSE-SU-2013:1089-1)	Vulnerability - level 2	Vuln
166064	SUSE Security Update for Subversion (openSUSE-SU-2013:1139-1)	Vulnerability - level 4	Vuln
166069	SUSE Security Update for openstack-swift (openSUSE-SU-2013:1146-1)	Vulnerability - level 4	Vuln
166079	SUSE Security Update for ruby19 (openSUSE-SU-2013:1179-1)	Vulnerability - level 3	Vuln
166081	SUSE Security Update for ruby19 (openSUSE-SU-2013:1181-1)	Vulnerability - level 3	Vuln
166082	SUSE Security Update for ruby19 (openSUSE-SU-2013:1186-1)	Vulnerability - level 3	Vuln
166083	SUSE Security Update for Kernel (openSUSE-SU-2013:1187-1)	Vulnerability - level 3	Vuln
166093	SUSE Security Update for php5 (openSUSE-SU-2013:1244-1)	Vulnerability - level 4	Vuln
166096	SUSE Security Update for php5 (openSUSE-SU-2013:1249-1)	Vulnerability - level 4	Vuln
166103	SUSE Security Update for Tomcat (openSUSE-SU-2013:1307-1)	Vulnerability - level 3	Vuln
166111	SUSE Security Update for apache2 (openSUSE-SU-2013:1337-1)	Vulnerability - level 3	Vuln
166112	SUSE Security Update for apache2 (openSUSE-SU-2013:1340-1)	Vulnerability - level 3	Vuln
166113	SUSE Security Update for apache2 (openSUSE-SU-2013:1341-1)	Vulnerability - level 3	Vuln
166116	SUSE Security Update for filezilla (openSUSE-SU-2013:1347-1)	Vulnerability - level 3	Vuln
166124	SUSE Security Update for openstack-keystone (openSUSE-SU-2013:0565-1)	Vulnerability - level 3	Vuln
166127	SUSE Security Update for Ruby (openSUSE-SU-2013:0603-1)	Vulnerability - level 4	Vuln
166128	SUSE Security Update for BIND (openSUSE-SU-2013:0605-1)	Vulnerability - level 4	Vuln
166133	SUSE Security Update for postgresql (openSUSE-SU-2013:0627-1)	Vulnerability - level 4	Vuln
166134	SUSE Security Update for postgresql (openSUSE-SU-2013:0628-1)	Vulnerability - level 4	Vuln
166135	SUSE Security Update for Apache2 (openSUSE-SU-2013:0629-1)	Vulnerability - level 2	Vuln
166138	SUSE Security Update for apache2 (openSUSE-SU-2013:0632-1)	Vulnerability - level 2	Vuln
166139	SUSE Security Update for postgresql (openSUSE-SU-2013:0635-1)	Vulnerability - level 4	Vuln
166146	SUSE Security Update for rubygem-actionpack-3_2 (openSUSE-SU-2013:0661-1)	Vulnerability - level 2	Vuln
166147	SUSE Security Update for rubygem-actionpack-2_3 (openSUSE-SU-2013:0662-1)	Vulnerability - level 2	Vuln
166149	SUSE Security Update for flash-player (openSUSE-SU-2013:0672-1)	Vulnerability - level 5	Vuln
166150	SUSE Security Update for flash-player (openSUSE-SU-2013:0675-1)	Vulnerability - level 5	Vuln
166171	SUSE Security Update for Samba (openSUSE-SU-2013:0277-1)	Vulnerability - level 3	Vuln
166175	SUSE Security Update for Samba (openSUSE-SU-2013:0281-1)	Vulnerability - level 3	Vuln
166194	SUSE Security Update for openssl (openSUSE-SU-2013:0336-1)	Vulnerability - level 4	Vuln
166216	SUSE Enterprise Linux Security Update for Real Time Linux Kernel (SUSE-SU-2013:1531-1)	Vulnerability - level 3	Vuln
166221	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2013:1474-1)	Vulnerability - level 4	Vuln
166222	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2013:1473-1)	Vulnerability - level 4	Vuln
166229	SUSE Enterprise Linux Security Update for Apache2 (SUSE-SU-2013:1381-1)	Vulnerability - level 3	Vuln
166231	SUSE Enterprise Linux Security Update for tomcat6 (SUSE-SU-2013:1374-1)	Vulnerability - level 3	Vuln

166234	SUSE Enterprise Linux Security Update for PHP5 (SUSE-SU-2013:1315-1)	Vulnerability - level 4	Vuln
166235	SUSE Enterprise Linux Security Update for PHP5 (SUSE-SU-2013:1317-1)	Vulnerability - level 4	Vuln
166236	SUSE Enterprise Linux Security Update for PHP5 (SUSE-SU-2013:1285-2)	Vulnerability - level 4	Vuln
166238	SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2013:1276-1)	Vulnerability - level 3	Vuln
166243	SUSE Enterprise Linux Security Update for Wireshark (SUSE-SU-2013:1265-1)	Vulnerability - level 3	Vuln
166252	SUSE Enterprise Linux Security Update for libcurl4 (SUSE-SU-2013:1165-1)	Vulnerability - level 3	Vuln
166254	SUSE Enterprise Linux Security Update for IBM Java (SUSE-SU-2013:0871-2)	Vulnerability - level 4	Vuln
166255	SUSE Enterprise Linux Security Update for IBM Java (SUSE-SU-2013:0835-3)	Vulnerability - level 4	Vuln
166257	SUSE Enterprise Linux Security Update for Java 1.4.2 (SUSE-SU-2013:0934-1)	Vulnerability - level 4	Vuln
166258	SUSE Enterprise Linux Security Update for IBM Java 1.7.0 (SUSE-SU-2013:0871-1)	Vulnerability - level 4	Vuln
166259	SUSE Enterprise Linux Security Update for Java 1.5.0 (SUSE-SU-2013:0835-2)	Vulnerability - level 4	Vuln
166262	SUSE Enterprise Linux Security Update for Subversion (SUSE-SU-2013:0837-1)	Vulnerability - level 3	Vuln
166264	SUSE Enterprise Linux Security Update for java-1_6_0-openjdk (SUSE-SU-2013:0814-1)	Vulnerability - level 4	Vuln
166267	SUSE Enterprise Linux Security Update for Ruby On Rails 3.2 stack (SUSE-SU-2013:0707-2)	Vulnerability - level 3	Vuln
166270	SUSE Enterprise Linux Security Update for Linux kernel (SUSE-SU-2013:0759-2)	Vulnerability - level 4	Vuln
166271	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2013:0744-1)	Vulnerability - level 3	Vuln
166272	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2013:1627-1)	Vulnerability - level 4	Vuln
166284	OpenSuSE Security Update for gpg2 (openSUSE-SU-2013:1546-1)	Vulnerability - level 3	Vuln
166289	OpenSuSE Security Update for gpg2 (openSUSE-SU-2013:1552-1)	Vulnerability - level 3	Vuln
166303	OpenSuSE Security Update for ruby19 (openSUSE-SU-2013:1611-1)	Vulnerability - level 3	Vuln
166308	OpenSuSE Security Update for Kernel (openSUSE-SU-2013:1619-1)	Vulnerability - level 3	Vuln
166341	OpenSuSE Security Update for XEN (openSUSE-SU-2013:1404-1)	Vulnerability - level 3	Vuln
166343	OpenSuSE Security Update for Tomcat (openSUSE-SU-2013:1411-1)	Vulnerability - level 3	Vuln
166379	OpenSuSE Security Update for Subversion (openSUSE-SU-2013:1286-1)	Vulnerability - level 3	Vuln
166387	OpenSuSE Security Update for Tomcat (openSUSE-SU-2013:1307-1)	Vulnerability - level 3	Vuln
166397	OpenSuSE Security Update for apache2 (openSUSE-SU-2013:1337-1)	Vulnerability - level 3	Vuln
166399	OpenSuSE Security Update for apache2 (openSUSE-SU-2013:1340-1)	Vulnerability - level 3	Vuln
166400	OpenSuSE Security Update for apache2 (openSUSE-SU-2013:1341-1)	Vulnerability - level 3	Vuln
166403	OpenSuSE Security Update for Filezilla (openSUSE-SU-2013:1347-1)	Vulnerability - level 3	Vuln
166408	OpenSuSE Security Update for Putty (openSUSE-SU-2013:1355-1)	Vulnerability - level 3	Vuln
166416	OpenSuSE Security Update for Fix kpasswd UDP ping-pong (openSUSE-SU-2013:1119-1)	Vulnerability - level 3	Vuln
166419	OpenSuSE Security Update for krb5 (openSUSE-SU-2013:1122-1)	Vulnerability - level 3	Vuln
166422	OpenSuSE Security Update for Subversion (openSUSE-SU-2013:1139-1)	Vulnerability - level 3	Vuln

166427	OpenSuSE Security Update for openstack-swift (openSUSE-SU-2013:1146-1)	Vulnerability - level 3	Vuln
166433	OpenSuSE Security Update for ruby19 (openSUSE-SU-2013:1179-1)	Vulnerability - level 3	Vuln
166436	OpenSuSE Security Update for ruby19 (openSUSE-SU-2013:1186-1)	Vulnerability - level 3	Vuln
166437	OpenSuSE Security Update for 3.0.80 Kernel Update (openSUSE-SU-2013:1187-1)	Vulnerability - level 4	Vuln
166451	OpenSuSE Security Update for php5 (openSUSE-SU-2013:1244-1)	Vulnerability - level 3	Vuln
166455	OpenSuSE Security Update for php5 (openSUSE-SU-2013:1249-1)	Vulnerability - level 3	Vuln
166459	OpenSuSE Security Update for strongswan (openSUSE-SU-2013:0873-1)	Vulnerability - level 3	Vuln
166462	OpenSuSE Security Update for xorg-x11-server (openSUSE-SU-2013:0878-1)	Vulnerability - level 3	Vuln
166467	OpenSuSE Security Update for libvirt (openSUSE-SU-2013:0885-1)	Vulnerability - level 3	Vuln
166474	OpenSuSE Security Update for wireshark (openSUSE-SU-2013:0911-1)	Vulnerability - level 4	Vuln
166478	OpenSuSE Security Update for tiff (openSUSE-SU-2013:0922-1)	Vulnerability - level 5	Vuln
166479	OpenSuSE Security Update for kernel (openSUSE-SU-2013:0923-1)	Vulnerability - level 4	Vuln
166480	OpenSuSE Security Update for kernel (openSUSE-SU-2013:0925-1)	Vulnerability - level 4	Vuln
166481	OpenSuSE Security Update for update kernel to 3.0 (openSUSE-SU-2013:0927-1)	Vulnerability - level 4	Vuln
166483	OpenSuSE Security Update for subversion (openSUSE-SU-2013:0932-1)	Vulnerability - level 3	Vuln
166485	OpenSuSE Security Update for xorg-x11-server (openSUSE-SU-2013:0937-1)	Vulnerability - level 2	Vuln
166487	OpenSuSE Security Update for wireshark (openSUSE-SU-2013:0947-1)	Vulnerability - level 4	Vuln
166498	OpenSuSE Security Update for wireshark (openSUSE-SU-2013:0848-1)	Vulnerability - level 4	Vuln
166501	OpenSuSE Security Update for ruby (openSUSE-SU-2013:0614-1)	Vulnerability - level 3	Vuln
166502	OpenSuSE Security Update for dhcp (openSUSE-SU-2013:0619-1)	Vulnerability - level 4	Vuln
166503	OpenSuSE Security Update for dhcp (openSUSE-SU-2013:0620-1)	Vulnerability - level 4	Vuln
166504	OpenSuSE Security Update for dhcp (openSUSE-SU-2013:0625-1)	Vulnerability - level 4	Vuln
166505	OpenSuSE Security Update for rubygem-activerecord-3_2 (openSUSE-SU-2013:0659-1)	Vulnerability - level 3	Vuln
166506	OpenSuSE Security Update for rubygem-activerecord-2_3 (openSUSE-SU-2013:0660-1)	Vulnerability - level 3	Vuln
166507	OpenSuSE Security Update for rubygem-activesupport-2_3 (openSUSE-SU-2013:0664-1)	Vulnerability - level 3	Vuln
166508	OpenSuSE Security Update for bind (openSUSE-SU-2013:0666-1)	Vulnerability - level 4	Vuln
166509	OpenSuSE Security Update for rubygem-activerecord-2_3 (openSUSE-SU-2013:0667-1)	Vulnerability - level 3	Vuln
166510	OpenSuSE Security Update for rubygem-activesupport-2_3 (openSUSE-SU-2013:0668-1)	Vulnerability - level 3	Vuln
166511	OpenSuSE Security Update for subversion (openSUSE-SU-2013:0687-1)	Vulnerability - level 3	Vuln
166512	OpenSuSE Security Update for wireshark (openSUSE-SU-2013:0494-1)	Vulnerability - level 4	Vuln
166514	OpenSuSE Security Update for wireshark (openSUSE-SU-2013:0506-1)	Vulnerability - level 3	Vuln
166518	OpenSuSE Security Update for libxml2 (openSUSE-SU-2013:0552-1)	Vulnerability - level 2	Vuln
166519	OpenSuSE Security Update for libxml2 (openSUSE-SU-2013:0555-1)	Vulnerability - level 3	Vuln
166522	OpenSuSE Security Update for openssl to 1.0.1e (openSUSE-SU-2013:0337-1)	Vulnerability - level 3	Vuln
166523	OpenSuSE Security Update for openssl (openSUSE-SU-2013:0339-1)	Vulnerability - level 3	Vuln
166538	OpenSuSE Security Update for 3.0.93 kernel Evergreen 11.4 (openSUSE-SU-2013:1773-1)	Vulnerability - level 3	Vuln

166539	OpenSUSE Security Update for chromium (openSUSE-SU-2013:1776-1)	Vulnerability - level 5	Vuln
166540	OpenSUSE Security Update for chromium (openSUSE-SU-2013:1777-1)	Vulnerability - level 5	Vuln
166552	OpenSUSE Security Update for subversion (openSUSE-SU-2013:1836-1)	Vulnerability - level 2	Vuln
166553	SUSE Enterprise Linux Security update for Linux kernel (SUSE-SU-2013:1832-1)	Vulnerability - level 4	Vuln
166555	SUSE Enterprise Linux Security update for Apache2 (SUSE-SU-2013:1824-1)	Vulnerability - level 3	Vuln
166564	SUSE Enterprise Linux Security update for libxslt (SUSE-SU-2013:1656-1)	Vulnerability - level 3	Vuln
166565	SUSE Enterprise Linux Security update for libxslt (SUSE-SU-2013:1654-1)	Vulnerability - level 3	Vuln
166571	SUSE Enterprise Linux Security update for libtiff (SUSE-SU-2013:1639-1)	Vulnerability - level 5	Vuln
166577	OpenSUSE Security Update for Subversion (openSUSE-SU-2013:1860-1)	Vulnerability - level 3	Vuln
166578	OpenSUSE Security Update for Chromium (openSUSE-SU-2013:1861-1)	Vulnerability - level 4	Vuln
166584	OpenSUSE Security Update for Subversion (openSUSE-SU-2013:1869-1)	Vulnerability - level 3	Vuln
166586	OpenSUSE Security Update for Mozilla Updates 2013/12 (openSUSE-SU-2013:1871-1)	Vulnerability - level 4	Vuln
166595	OpenSUSE Security Update for Mozilla Firefox (openSUSE-SU-2013:1916-1)	Vulnerability - level 3	Vuln
166596	OpenSUSE Security Update for Mozilla Firefox (openSUSE-SU-2013:1917-1)	Vulnerability - level 3	Vuln
166597	OpenSUSE Security Update for Mozilla Firefox (openSUSE-SU-2013:1918-1)	Vulnerability - level 3	Vuln
166607	SUSE Enterprise Linux Security Update for Real Time Linux Kernel (SUSE-SU-2014:0168-1)	Vulnerability - level 3	Vuln
166608	SUSE Enterprise Linux Security Update for Real Time Linux Kernel (SUSE-SU-2014:0169-1)	Vulnerability - level 3	Vuln
166617	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2014:0140-1)	Vulnerability - level 3	Vuln
166618	SUSE Enterprise Linux Security Update for Subversion (SUSE-SU-2014:0129-1)	Vulnerability - level 3	Vuln
166626	SUSE Enterprise Linux Security Update for lighttpd (SUSE-SU-2014:0050-1)	Vulnerability - level 4	Vuln
166634	SUSE Enterprise Linux Security Update for apache2-mod_nss (SUSE-SU-2013:1926-1)	Vulnerability - level 2	Vuln
166636	SUSE Enterprise Linux Security Update for Xen (SUSE-SU-2013:1923-1)	Vulnerability - level 4	Vuln
166646	SUSE Enterprise Linux Security Update for java-1_6_0-ibm (SUSE-SU-2013:0701-2)	Vulnerability - level 5	Vuln
166648	SUSE Enterprise Linux Security Update for java-1_7_0-ibm (SUSE-SU-2013:0701-1)	Vulnerability - level 5	Vuln
166650	SUSE Enterprise Linux Security Update for OpenSSL (SUSE-SU-2013:0549-2)	Vulnerability - level 3	Vuln
166675	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2014:0189-1)	Vulnerability - level 3	Vuln
166687	SUSE Enterprise Linux Security update for rubygem-activesupport-2_3 (SUSE-SU-2013:0209-1)	Vulnerability - level 2	Vuln
166688	SUSE Enterprise Linux Security update for hawk (SUSE-SU-2013:0194-1)	Vulnerability - level 3	Vuln
166697	SUSE Enterprise Linux Security Update for Mozilla Firefox (SUSE-SU-2014:0248-2)	Vulnerability - level 4	Vuln

166698	SUSE Enterprise Linux Security Update for Mozilla Firefox (SUSE-SU-2014:0248-1)	Vulnerability - level 4	Vuln
166703	OpenSUSE Security Update for Seamonkey (openSUSE-SU-2014:0008-1)	Vulnerability - level 3	Vuln
166707	OpenSUSE Security Update for OpenSSL (openSUSE-SU-2014:0012-1)	Vulnerability - level 3	Vuln
166710	OpenSUSE Security Update for OpenSSL (openSUSE-SU-2014:0015-1)	Vulnerability - level 3	Vuln
166713	OpenSUSE Security Update for OpenSSL (openSUSE-SU-2014:0018-1)	Vulnerability - level 3	Vuln
166714	OpenSUSE Security Update for rubygem-actionpack-2_3 (openSUSE-SU-2014:0019-1)	Vulnerability - level 3	Vuln
166718	OpenSUSE Security Update for OpenSSL (openSUSE-SU-2014:0048-1)	Vulnerability - level 3	Vuln
166719	OpenSUSE Security Update for OpenSSL (openSUSE-SU-2014:0049-1)	Vulnerability - level 3	Vuln
166720	OpenSUSE Security Update for chromium (openSUSE-SU-2014:0065-1)	Vulnerability - level 3	Vuln
166730	OpenSUSE Security Update for OpenSSL (openSUSE-SU-2014:0094-1)	Vulnerability - level 3	Vuln
166731	OpenSUSE Security Update for OpenSSL (openSUSE-SU-2014:0096-1)	Vulnerability - level 3	Vuln
166733	OpenSUSE Security Update for openssl (openSUSE-SU-2014:0099-1)	Vulnerability - level 3	Vuln
166761	OpenSUSE Security Update for Kernel (openSUSE-SU-2014:0204-1)	Vulnerability - level 4	Vuln
166763	OpenSUSE Security Update for Mozilla Firefox (openSUSE-SU-2014:0212-1)	Vulnerability - level 4	Vuln
166769	OpenSUSE Security Update for Kernel (openSUSE-SU-2014:0247-1)	Vulnerability - level 3	Vuln
166780	OpenSUSE Security Update for rubygem-actionpack-3_2 (openSUSE-SU-2014:0295-1)	Vulnerability - level 3	Vuln
166783	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2014:0287-1)	Vulnerability - level 3	Vuln
166790	SUSE Enterprise Linux Security Update for OpenSSL (SUSE-SU-2014:0541-1)	Vulnerability - level 3	Vuln
166791	SUSE Enterprise Linux Security Update for OpenSSL (SUSE-SU-2014:0538-1)	Vulnerability - level 3	Vuln
166792	SUSE Enterprise Linux Security Update for OpenSSL (SUSE-SU-2014:0539-1)	Vulnerability - level 3	Vuln
166793	SUSE Enterprise Linux Security update for Linux Kernel (SUSE-SU-2014:0537-1)	Vulnerability - level 4	Vuln
166794	SUSE Enterprise Linux Security Update for flash-player (SUSE-SU-2014:0535-1)	Vulnerability - level 4	Vuln
166795	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2014:0536-1)	Vulnerability - level 4	Vuln
166796	SUSE Enterprise Linux Security update for Linux Kernel (SUSE-SU-2014:0531-1)	Vulnerability - level 4	Vuln
166808	SUSE Enterprise Linux Security Update for Xen (SUSE-SU-2014:0470-1)	Vulnerability - level 4	Vuln
166811	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2014:0459-1)	Vulnerability - level 4	Vuln
166813	SUSE Enterprise Linux Security Update for Xen (SUSE-SU-2014:0446-1)	Vulnerability - level 4	Vuln
166817	SUSE Enterprise Linux Security Update for libssh2 (SUSE-SU-2014:0413-1)	Vulnerability - level 3	Vuln
166818	SUSE Enterprise Linux Security Update for Xen (SUSE-SU-2014:0411-1)	Vulnerability - level 4	Vuln
166821	SUSE Enterprise Linux Security Update for Xen (SUSE-SU-2014:0372-1)	Vulnerability - level 4	Vuln

166822	SUSE Enterprise Linux Security Update for Xen (SUSE-SU-2014:0373-1)	Vulnerability - level 4	Vuln
166826	SUSE Enterprise Linux Security Update for python (SUSE-SU-2014:0337-1)	Vulnerability - level 3	Vuln
166830	SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2014:0320-1)	Vulnerability - level 5	Vuln
166831	SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2014:0321-1)	Vulnerability - level 5	Vuln
166832	SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2014:0322-1)	Vulnerability - level 5	Vuln
166833	SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2014:0323-1)	Vulnerability - level 5	Vuln
166834	SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2014:0319-1)	Vulnerability - level 5	Vuln
166838	OpenSuSE Security Update for gnutls (openSUSE-SU-2014:0325-1)	Vulnerability - level 5	Vuln
166841	OpenSuSE Security Update for gnutls (openSUSE-SU-2014:0328-1)	Vulnerability - level 5	Vuln
166848	OpenSuSE Security Update for gnutls (openSUSE-SU-2014:0346-1)	Vulnerability - level 5	Vuln
166858	OpenSuSE Security Update for libssh (openSUSE-SU-2014:0366-1)	Vulnerability - level 3	Vuln
166862	OpenSuSE Security Update for libssh (openSUSE-SU-2014:0370-1)	Vulnerability - level 3	Vuln
166885	OpenSuSE Security Update for nginx (openSUSE-SU-2014:0450-1)	Vulnerability - level 3	Vuln
166887	SUSE Enterprise Linux Security Update for gpg2 (SUSE-SU-2014:0750-1)	Vulnerability - level 3	Vuln
166888	SUSE Enterprise Linux Security update for IBM Java 6 (SUSE-SU-2014:0728-3)	Vulnerability - level 4	Vuln
166889	SUSE Enterprise Linux Security Update for xorg-x11-server (SUSE-SU-2014:0744-1)	Vulnerability - level 3	Vuln
166890	SUSE Enterprise Linux Security Update for IBM Java 7 (SUSE-SU-2014:0733-2)	Vulnerability - level 4	Vuln
166891	SUSE Enterprise Linux Security Update for IBM Java 7 (SUSE-SU-2014:0733-1)	Vulnerability - level 4	Vuln
166892	SUSE Enterprise Linux Security Update for IBM Java 6 (SUSE-SU-2014:0728-2)	Vulnerability - level 4	Vuln
166893	SUSE Enterprise Linux Security Update for IBM Java 5 (SUSE-SU-2014:0732-1)	Vulnerability - level 3	Vuln
166896	SUSE Enterprise Linux Security Update for Samba (SUSE-SU-2014:0723-1)	Vulnerability - level 3	Vuln
166897	SUSE Enterprise Linux Security Update for libpng (SUSE-SU-2014:0724-1)	Vulnerability - level 3	Vuln
166901	SUSE Enterprise Linux Security Update for Linux kernel (SUSE-SU-2014:0696-1)	Vulnerability - level 4	Vuln
166902	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2014:0691-1)	Vulnerability - level 3	Vuln
166903	SUSE Enterprise Linux Security Update for Ruby (SUSE-SU-2014:0689-1)	Vulnerability - level 3	Vuln
166913	SUSE Enterprise Linux Security Update for OpenJDK (SUSE-SU-2014:0639-1)	Vulnerability - level 4	Vuln
166929	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2014:0759-2)	Vulnerability - level 5	Vuln
166930	SUSE Enterprise Linux Security update for MySQL (SUSE-SU-2014:0769-1)	Vulnerability - level 4	Vuln
166932	OpenSuSE Security Update for openssl (openSUSE-SU-2014:0480-1)	Vulnerability - level 3	Vuln
166934	OpenSuSE Security Update for xen (openSUSE-SU-2014:0482-1)	Vulnerability - level 3	Vuln
166935	OpenSuSE Security Update for xen (openSUSE-SU-2014:0483-1)	Vulnerability - level 3	Vuln
166949	OpenSuSE Security Update for flash-player (openSUSE-SU-2014:0520-1)	Vulnerability - level 3	Vuln
166953	OpenSuSE Security Update for curl (openSUSE-SU-2014:0530-1)	Vulnerability - level 3	Vuln
166954	OpenSuSE Security Update for flash-player (openSUSE-SU-2014:0549-1)	Vulnerability - level 3	Vuln

166955	OpenSuSE Security Update for json-c (openSUSE-SU-2014:0558-1)	Vulnerability - level 3	Vuln
166964	OpenSuSE Security Update for OpenSSL (openSUSE-SU-2014:0592-1)	Vulnerability - level 3	Vuln
166970	OpenSuSE Security Update for curl (openSUSE-SU-2014:0598-1)	Vulnerability - level 3	Vuln
166976	OpenSuSE Security Update for libpng12 (openSUSE-SU-2014:0604-1)	Vulnerability - level 3	Vuln
166978	OpenSuSE Security Update for libpng15 (openSUSE-SU-2014:0616-1)	Vulnerability - level 3	Vuln
166979	OpenSuSE Security Update for libpng12 (openSUSE-SU-2014:0618-1)	Vulnerability - level 3	Vuln
166983	OpenSuSE Security Update for openssl (openSUSE-SU-2014:0634-1)	Vulnerability - level 3	Vuln
166984	OpenSuSE Security Update for Openssl (openSUSE-SU-2014:0635-1)	Vulnerability - level 3	Vuln
166994	OpenSuSE Security Update for Kernel (openSUSE-SU-2014:0677-1)	Vulnerability - level 4	Vuln
166995	OpenSuSE Security Update for Kernel (openSUSE-SU-2014:0678-1)	Vulnerability - level 4	Vuln
167017	OpenSuSE Security Update for Openssl (openSUSE-SU-2014:0764-1)	Vulnerability - level 5	Vuln
167018	OpenSuSE Security Update for Openssl (openSUSE-SU-2014:0765-1)	Vulnerability - level 5	Vuln
167019	OpenSuSE Security Update for Kernel (openSUSE-SU-2014:0766-1)	Vulnerability - level 3	Vuln
167108	OpenSuSE Security Update for elfutils (openSUSE-SU-2014:0974-1)	Vulnerability - level 2	Vuln
167135	OpenSuSE Security Update for openssl (openSUSE-SU-2014:1052-1)	Vulnerability - level 3	Vuln
167161	SUSE Enterprise Linux Security Update for LibreOffice (SUSE-SU-2014:1116-1)	Vulnerability - level 4	Vuln
167165	SUSE Enterprise Linux Security Update for OpenSSL (SUSE-SU-2014:1104-1)	Vulnerability - level 3	Vuln
167168	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2014:1082-1)	Vulnerability - level 4	Vuln
167176	SUSE Enterprise Linux Security Update for OpenSSL (SUSE-SU-2014:1049-1)	Vulnerability - level 3	Vuln
167184	SUSE Enterprise Linux Security Update for tomcat6 (SUSE-SU-2014:1015-1)	Vulnerability - level 3	Vuln
167213	SUSE Enterprise Linux Security Update for ruby (SUSE-SU-2014:0843-1)	Vulnerability - level 3	Vuln
167214	SUSE Enterprise Linux Security Update for ruby (SUSE-SU-2014:0844-1)	Vulnerability - level 3	Vuln
167221	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2014:0832-1)	Vulnerability - level 3	Vuln
167228	SUSE Enterprise Linux Security Update for Linux Kernel (SUSE-SU-2014:0807-1)	Vulnerability - level 4	Vuln
167244	OpenSuSE Security Update for LibreOffice (openSUSE-SU-2014:1126-1)	Vulnerability - level 4	Vuln
167246	OpenSuSE Security Update for python-django (openSUSE-SU-2014:1132-1)	Vulnerability - level 3	Vuln
167259	OpenSuSE Security Update for dbus-1 (openSUSE-SU-2014:1239-1)	Vulnerability - level 3	Vuln
167276	OpenSuSE Security Update for dbus-1 (openSUSE-SU-2014:1228-1)	Vulnerability - level 3	Vuln
167302	SUSE Enterprise Linux Security update for Linux kernel (SUSE-SU-2014:1319-1)	Vulnerability - level 4	Vuln
167303	SUSE Enterprise Linux Security update for Linux kernel (SUSE-SU-2014:1316-1)	Vulnerability - level 4	Vuln
167314	OpenSuSE Security Update for docker (openSUSE-SU-2014:1596-1)	Vulnerability - level 4	Vuln
167323	OpenSuSE Security Update for java-1_7_0-openjdk (openSUSE-SU-2014:1638-1)	Vulnerability - level 3	Vuln
167328	OpenSuSE Security Update for java-1_7_0-openjdk (openSUSE-SU-2014:1645-1)	Vulnerability - level 3	Vuln

167330	OpenSuSE Security Update for apache2 (openSUSE-SU-2014:1647-1)	Vulnerability - level 3	Vuln
167334	OpenSuSE Security Update for Linux Kernel (openSUSE-SU-2014:1669-1)	Vulnerability - level 4	Vuln
167336	OpenSuSE Security Update for Linux Kernel (openSUSE-SU-2014:1677-1)	Vulnerability - level 4	Vuln
167337	OpenSuSE Security Update for Linux Kernel (openSUSE-SU-2014:1678-1)	Vulnerability - level 4	Vuln
167340	OpenSuSE Security Update for libksba (openSUSE-SU-2014:1682-1)	Vulnerability - level 3	Vuln
167342	OpenSuSE Security Update for unbound (openSUSE-SU-2014:1688-1)	Vulnerability - level 3	Vuln
167349	OpenSuSE Security Update for subversion (openSUSE-SU-2014:1725-1)	Vulnerability - level 3	Vuln
167354	OpenSuSE Security Update for kernel (openSUSE-SU-2014:1735-1)	Vulnerability - level 4	Vuln
167371	OpenSuSE Security Update for ImageMagick (openSUSE-SU-2014:1396-1)	Vulnerability - level 3	Vuln
167375	OpenSuSE Security Update for docker, go (openSUSE-SU-2014:1411-1)	Vulnerability - level 3	Vuln
167402	SUSE Enterprise Linux Security update for dbus-1 (SUSE-SU-2014:1724-1)	Vulnerability - level 1	Vuln
167410	SUSE Enterprise Linux Security update for Linux kernel (SUSE-SU-2014:1698-1)	Vulnerability - level 4	Vuln
167411	SUSE Enterprise Linux Security update for Linux kernel (SUSE-SU-2014:1695-1)	Vulnerability - level 4	Vuln
167417	SUSE Enterprise Linux Security update for libksba (SUSE-SU-2014:1676-1)	Vulnerability - level 2	Vuln
167424	SUSE Enterprise Linux Security update for Image Magick (SUSE-SU-2014:1631-1)	Vulnerability - level 3	Vuln
167430	SUSE Enterprise Linux Security update for ImageMagick (SUSE-SU-2014:1595-1)	Vulnerability - level 3	Vuln
167437	SUSE Enterprise Linux Security update for compat-openssl097g (SUSE-SU-2014:1557-2)	Vulnerability - level 3	Vuln
167486	OpenSuSE Security Update for jasper (openSUSE-SU-2015:0038-1)	Vulnerability - level 3	Vuln
167487	OpenSuSE Security Update for jasper (openSUSE-SU-2015:0039-1)	Vulnerability - level 3	Vuln
167489	OpenSuSE Security Update for jasper (openSUSE-SU-2015:0042-1)	Vulnerability - level 3	Vuln
167494	OpenSuSE Security Update for MozillaFirefox (openSUSE-SU-2015:0077-1)	Vulnerability - level 4	Vuln
167497	OpenSuSE Security Update for MozillaFirefox (openSUSE-SU-2015:0077-2)	Vulnerability - level 4	Vuln
167505	OpenSuSE Security Update for openssl (openSUSE-SU-2015:0130-1)	Vulnerability - level 4	Vuln
167518	SUSE Enterprise Linux Security update for compat-openssl097g (SUSE-SU-2015:0182-1)	Vulnerability - level 3	Vuln
167519	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:0172-2)	Vulnerability - level 3	Vuln
167520	SUSE Enterprise Linux Security update for Mozilla Firefox (SUSE-SU-2015:0180-1)	Vulnerability - level 4	Vuln
167521	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2015:0205-1)	Vulnerability - level 3	Vuln
167522	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:0172-1)	Vulnerability - level 3	Vuln
167523	SUSE Enterprise Linux Security update for Mozilla Firefox (SUSE-SU-2015:0171-1)	Vulnerability - level 4	Vuln
167524	SUSE Enterprise Linux Security update for Mozilla Firefox (SUSE-SU-2015:0173-1)	Vulnerability - level 4	Vuln
167533	SUSE Enterprise Linux Security update for subversion (SUSE-SU-2015:0155-2)	Vulnerability - level 2	Vuln

167541	SUSE Enterprise Linux Security update for curl (SUSE-SU-2015:0083-1)	Vulnerability - level 2	Vuln
167544	SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2015:0068-1)	Vulnerability - level 4	Vuln
167550	SUSE Enterprise Linux Security update for Linux kernel (SUSE-SU-2014:1695-2)	Vulnerability - level 4	Vuln
167552	SUSE Enterprise Linux Security update for libksba (SUSE-SU-2015:0030-1)	Vulnerability - level 3	Vuln
167558	SUSE Enterprise Linux Security update for jasper (SUSE-SU-2015:0016-1)	Vulnerability - level 4	Vuln
167559	SUSE Enterprise Linux Security update for subversion (SUSE-SU-2015:0153-1)	Vulnerability - level 3	Vuln
167562	SUSE Enterprise Linux Security update for xntp (SUSE-SU-2015:0322-1)	Vulnerability - level 4	Vuln
167565	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2015:0259-3)	Vulnerability - level 4	Vuln
167566	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2015:0259-1)	Vulnerability - level 4	Vuln
167567	SUSE Enterprise Linux Security update for jasper (SUSE-SU-2015:0258-1)	Vulnerability - level 3	Vuln
167571	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2015:0274-1)	Vulnerability - level 4	Vuln
167574	SUSE Enterprise Linux Security update for compat-openssl098 (SUSE-SU-2015:0305-1)	Vulnerability - level 3	Vuln
167588	OpenSUSE Security Update for seamonkey (openSUSE-SU-2015:0192-1)	Vulnerability - level 4	Vuln
167602	OpenSUSE Security Update for curl (openSUSE-SU-2015:0248-1)	Vulnerability - level 3	Vuln
167645	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2015:0259-2)	Vulnerability - level 3	Vuln
167672	OpenSUSE Security Update for openssl (openSUSE-SU-2015:0554-1)	Vulnerability - level 3	Vuln
167673	OpenSUSE Security Update for kernel (openSUSE-SU-2015:0566-1)	Vulnerability - level 4	Vuln
167686	SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2015:0581-1)	Vulnerability - level 4	Vuln
167688	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:0545-2)	Vulnerability - level 3	Vuln
167691	SUSE Enterprise Linux Security update for compat-openssl097g (SUSE-SU-2015:0548-1)	Vulnerability - level 3	Vuln
167692	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:0549-1)	Vulnerability - level 3	Vuln
167693	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:0545-1)	Vulnerability - level 3	Vuln
167694	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:0547-1)	Vulnerability - level 3	Vuln
167695	SUSE Enterprise Linux Security update for compat-openssl098 (SUSE-SU-2015:0553-2)	Vulnerability - level 4	Vuln
167696	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2015:0541-1)	Vulnerability - level 3	Vuln
167714	OpenSUSE Security Update for subversion (openSUSE-SU-2015:0672-1)	Vulnerability - level 3	Vuln
167733	SUSE Enterprise Linux Security update for Real Time Linux Kernel (SUSE-SU-2015:0736-1)	Vulnerability - level 4	Vuln
167737	SUSE Enterprise Linux Security update for subversion (SUSE-SU-2015:0709-1)	Vulnerability - level 3	Vuln
167764	SUSE Enterprise Linux Security update for mariadb (SUSE-SU-2015:0743-1)	Vulnerability - level 4	Vuln
167785	SUSE Enterprise Linux Security update for Linux Kernel (SUSE-SU-2015:0812-1)	Vulnerability - level 4	Vuln

167788	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2015:0865-1)	Vulnerability - level 2	Vuln
167792	SUSE Enterprise Linux Security update for subversion (SUSE-SU-2015:0776-1)	Vulnerability - level 4	Vuln
167806	OpenSUSE Security Update for ntp (openSUSE-SU-2015:0775-1)	Vulnerability - level 3	Vuln
167810	OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2015:0813-1)	Vulnerability - level 4	Vuln
167847	SUSE Enterprise Linux Security update for MySQL (SUSE-SU-2015:0946-1)	Vulnerability - level 3	Vuln
167874	SUSE Enterprise Linux Security update for MozillaFirefox, mozilla-nspr, mozilla-nss (SUSE-SU-2015:1269-1)	Vulnerability - level 5	Vuln
167877	SUSE Enterprise Linux Security update for MySQL (SUSE-SU-2015:1177-2)	Vulnerability - level 2	Vuln
167880	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:1183-2)	Vulnerability - level 3	Vuln
167881	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:1184-1)	Vulnerability - level 3	Vuln
167882	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:1182-2)	Vulnerability - level 3	Vuln
167883	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:1184-2)	Vulnerability - level 3	Vuln
167884	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2015:1181-2)	Vulnerability - level 3	Vuln
167885	SUSE Enterprise Linux Security update for MySQL (SUSE-SU-2015:1177-1)	Vulnerability - level 2	Vuln
167886	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2015:1173-1)	Vulnerability - level 2	Vuln
167890	SUSE Enterprise Linux Security update for java-1_7_0-ibm (SUSE-SU-2015:1086-4)	Vulnerability - level 5	Vuln
167893	SUSE Enterprise Linux Security update for Java (SUSE-SU-2015:1086-3)	Vulnerability - level 5	Vuln
167894	SUSE Enterprise Linux Security update for IBM Java (SUSE-SU-2015:1138-1)	Vulnerability - level 5	Vuln
167900	SUSE Enterprise Linux Security update for IBM Java (SUSE-SU-2015:1086-2)	Vulnerability - level 5	Vuln
167902	SUSE Enterprise Linux Security update for IBM Java (SUSE-SU-2015:1086-1)	Vulnerability - level 5	Vuln
167903	SUSE Enterprise Linux Security update for IBM Java (SUSE-SU-2015:1085-1)	Vulnerability - level 5	Vuln
167904	SUSE Enterprise Linux Security update for compat-openssl098 (SUSE-SU-2015:1150-1)	Vulnerability - level 3	Vuln
167905	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2015:1143-1)	Vulnerability - level 3	Vuln
167907	SUSE Enterprise Linux Security update for java-1_7_0-ibm (SUSE-SU-2015:1073-1)	Vulnerability - level 5	Vuln
167925	SUSE Enterprise Linux Security update for wpa_supplicant (SUSE-SU-2015:1013-1)	Vulnerability - level 3	Vuln
167950	OpenSUSE Security Update for openssl (openSUSE-SU-2015:1139-1)	Vulnerability - level 4	Vuln
167959	OpenSUSE Security Update for mysql-community-server (openSUSE-SU-2015:1209-1)	Vulnerability - level 3	Vuln
167965	OpenSUSE Security Update for MariaDB (openSUSE-SU-2015:1216-1)	Vulnerability - level 4	Vuln
167966	OpenSUSE Security Update for MozillaFirefox, mozilla-nss (openSUSE-SU-2015:1229-1)	Vulnerability - level 4	Vuln
167976	OpenSUSE Security Update for Mozilla (Firefox/Thunderbird) updates to 31.8.0 (openSUSE-SU-2015:1266-1)	Vulnerability - level 4	Vuln
167979	OpenSUSE Security Update for libressl (openSUSE-SU-2015:1277-1)	Vulnerability - level 4	Vuln

167983	OpenSUSE Security Update for Chromium (openSUSE-SU-2015:1287-1)	Vulnerability - level 4	Vuln
167984	OpenSUSE Security Update for java-1_7_0-openjdk (openSUSE-SU-2015:1288-1)	Vulnerability - level 4	Vuln
167985	OpenSUSE Security Update for java-1_8_0-openjdk (openSUSE-SU-2015:1289-1)	Vulnerability - level 4	Vuln
167997	SUSE Enterprise Linux Security update for tomcat6 (SUSE-SU-2015:1337-1)	Vulnerability - level 4	Vuln
167999	SUSE Enterprise Linux Security update for java-1_7_1-ibm (SUSE-SU-2015:1331-1)	Vulnerability - level 5	Vuln
168000	SUSE Enterprise Linux Security update for java-1_7_0-openjdk (SUSE-SU-2015:1319-1)	Vulnerability - level 5	Vuln
168039	SUSE Enterprise Linux Security update for openssh (SUSE-SU-2015:1544-1)	Vulnerability - level 4	Vuln
168055	SUSE Enterprise Linux Recommended update for openssl (SUSE-SU-2015:1410-1)	Vulnerability - level 3	Vuln
168064	SUSE Enterprise Linux Security update for openssh (SUSE-SU-2015:1581-1)	Vulnerability - level 4	Vuln
168065	SUSE Enterprise Linux Security update for tomcat6 (SUSE-SU-2015:1565-1)	Vulnerability - level 3	Vuln
168090	SUSE Enterprise Linux Security update for openssh (SUSE-SU-2015:1695-1)	Vulnerability - level 3	Vuln
168114	OpenSUSE Security Update for apache2 (openSUSE-SU-2015:1684-1)	Vulnerability - level 3	Vuln
168126	OpenSUSE Security Update for jakarta-taglibs-standard (openSUSE-SU-2015:1751-1)	Vulnerability - level 3	Vuln
168152	SUSE Enterprise Linux Security update for openssh (SUSE-SU-2015:1840-1)	Vulnerability - level 3	Vuln
168162	SUSE Enterprise Linux Security update for apache2 (SUSE-SU-2015:1851-1)	Vulnerability - level 3	Vuln
168183	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2015:2058-1)	Vulnerability - level 3	Vuln
168209	SUSE Enterprise Linux Security update for java-1_6_0-ibm (SUSE-SU-2015:2166-1)	Vulnerability - level 4	Vuln
168232	OpenSUSE Security Update for ntp (openSUSE-SU-2015:2016-1)	Vulnerability - level 3	Vuln
168254	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2015:2253-1)	Vulnerability - level 3	Vuln
168255	SUSE Enterprise Linux Security update for compat-openssl097g (SUSE-SU-2015:2251-1)	Vulnerability - level 3	Vuln
168257	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2015:2237-1)	Vulnerability - level 3	Vuln
168269	OpenSUSE Security Update for MySQL 5.6.27 (openSUSE-SU-2015:2243-1)	Vulnerability - level 4	Vuln
168279	OpenSUSE Security Update for OpenSSL (openSUSE-SU-2015:2288-1)	Vulnerability - level 3	Vuln
168280	OpenSUSE Security Update for openssl (openSUSE-SU-2015:2289-1)	Vulnerability - level 3	Vuln
168284	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2015:2275-1)	Vulnerability - level 3	Vuln
168287	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2015:2230-1)	Vulnerability - level 3	Vuln
168298	SUSE Enterprise Linux Security update for mysql (SUSE-SU-2015:2303-1)	Vulnerability - level 3	Vuln
168302	SUSE Enterprise Linux Security update for compat-openssl098 (SUSE-SU-2015:2342-1)	Vulnerability - level 3	Vuln
168316	OpenSUSE Security Update for libressl (openSUSE-SU-2015:2318-1)	Vulnerability - level 3	Vuln
168319	OpenSUSE Security Update for compat-openssl098 (openSUSE-SU-2015:2349-1)	Vulnerability - level 3	Vuln

168370	SUSE Enterprise Linux Security update for java-1_6_0-ibm (SUSE-SU-2016:0113-1)	Vulnerability - level 4	Vuln
168386	OpenSUSE Security Update for gajim (openSUSE-SU-2016:0102-1)	Vulnerability - level 3	Vuln
168419	SUSE Enterprise Linux Security update for openldap2 (SUSE-SU-2016:0224-1)	Vulnerability - level 4	Vuln
168452	OpenSUSE Security Update for jasper (openSUSE-SU-2016:0217-1)	Vulnerability - level 2	Vuln
168454	OpenSUSE Security Update for openldap2 (openSUSE-SU-2016:0226-1)	Vulnerability - level 4	Vuln
168461	OpenSUSE Security Update for openldap2 (openSUSE-SU-2016:0255-1)	Vulnerability - level 4	Vuln
168462	OpenSUSE Security Update for openldap2 (openSUSE-SU-2016:0261-1)	Vulnerability - level 4	Vuln
168480	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2016:0301-1)	Vulnerability - level 4	Vuln
168493	OpenSUSE Security Update for openssl (openSUSE-SU-2016:0362-1)	Vulnerability - level 2	Vuln
168517	OpenSUSE Security Update for openssl (openSUSE-SU-2016:0442-1)	Vulnerability - level 2	Vuln
168521	OpenSUSE Security Update for socat (openSUSE-SU-2016:0478-1)	Vulnerability - level 3	Vuln
168523	OpenSUSE Security Update for socat (openSUSE-SU-2016:0483-1)	Vulnerability - level 3	Vuln
168544	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2016:0620-1)	Vulnerability - level 4	Vuln
168545	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2016:0617-1)	Vulnerability - level 4	Vuln
168546	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2016:0641-1)	Vulnerability - level 4	Vuln
168548	SUSE Enterprise Linux Security update for compat-openssl097g (SUSE-SU-2016:0631-1)	Vulnerability - level 4	Vuln
168550	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2016:0624-1)	Vulnerability - level 4	Vuln
168552	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2016:0621-1)	Vulnerability - level 4	Vuln
168554	SUSE Enterprise Linux Security update for OpenSSL (SUSE-SU-2016:0678-1)	Vulnerability - level 4	Vuln
168570	SUSE Enterprise Linux Security update for tomcat (SUSE-SU-2016:0769-1)	Vulnerability - level 4	Vuln
168576	SUSE Enterprise Linux Security update for tomcat6 (SUSE-SU-2016:0839-1)	Vulnerability - level 4	Vuln
168578	SUSE Enterprise Linux Security update for tomcat (SUSE-SU-2016:0822-1)	Vulnerability - level 4	Vuln
168588	SUSE Enterprise Linux Security update for xerces-c (SUSE-SU-2016:1026-1)	Vulnerability - level 3	Vuln
168622	OpenSUSE Security Update for Security openssl (openSUSE-SU-2016:0627-1)	Vulnerability - level 4	Vuln
168623	OpenSUSE Security Update for Security openssl (openSUSE-SU-2016:0628-1)	Vulnerability - level 4	Vuln
168624	OpenSUSE Security Update for Security openssl (openSUSE-SU-2016:0637-1)	Vulnerability - level 4	Vuln
168625	OpenSUSE Security Update for Security openssl (openSUSE-SU-2016:0638-1)	Vulnerability - level 4	Vuln
168627	OpenSUSE Security Update for Security libopenssl0_9_8 (openSUSE-SU-2016:0640-1)	Vulnerability - level 4	Vuln
168643	OpenSUSE Security Update for Security openssl (openSUSE-SU-2016:0720-1)	Vulnerability - level 4	Vuln
168674	OpenSUSE Security Update for Security tomcat (openSUSE-SU-2016:0865-1)	Vulnerability - level 4	Vuln
168720	OpenSUSE Security Update for Security xerces-c (openSUSE-SU-2016:1121-1)	Vulnerability - level 3	Vuln

168747	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2016:1233-1)	Vulnerability - level 4	Vuln
168748	SUSE Enterprise Linux Security update for openssl1 (SUSE-SU-2016:1206-1)	Vulnerability - level 4	Vuln
168751	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2016:1175-1)	Vulnerability - level 4	Vuln
168763	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2016:1247-1)	Vulnerability - level 4	Vuln
168767	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2016:1228-1)	Vulnerability - level 4	Vuln
168774	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2016:1177-1)	Vulnerability - level 4	Vuln
168789	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2016:1278-1)	Vulnerability - level 4	Vuln
168791	SUSE Enterprise Linux Security update for compat-openssl098 (SUSE-SU-2016:1267-1)	Vulnerability - level 4	Vuln
168796	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2016:1291-1)	Vulnerability - level 4	Vuln
168797	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2016:1290-1)	Vulnerability - level 4	Vuln
168798	SUSE Enterprise Linux Security update for openssl (SUSE-SU-2016:1360-1)	Vulnerability - level 4	Vuln
168806	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2016:1311-1)	Vulnerability - level 4	Vuln
168829	OpenSUSE Security Update for openssl (openSUSE-SU-2016:1237-1)	Vulnerability - level 4	Vuln
168830	OpenSUSE Security Update for openssl (openSUSE-SU-2016:1238-1)	Vulnerability - level 4	Vuln
168831	OpenSUSE Security Update for libopenssl0_9_8 (openSUSE-SU-2016:1239-1)	Vulnerability - level 4	Vuln
168832	OpenSUSE Security Update for openssl (openSUSE-SU-2016:1240-1)	Vulnerability - level 4	Vuln
168833	OpenSUSE Security Update for libopenssl0_9_8 (openSUSE-SU-2016:1241-1)	Vulnerability - level 4	Vuln
168834	OpenSUSE Security Update for libopenssl0_9_8 (openSUSE-SU-2016:1242-1)	Vulnerability - level 4	Vuln
168835	OpenSUSE Security Update for openssl (openSUSE-SU-2016:1243-1)	Vulnerability - level 4	Vuln
168843	OpenSUSE Security Update for compat-openssl098 (openSUSE-SU-2016:1273-1)	Vulnerability - level 4	Vuln
168845	OpenSUSE Security Update for ntp (openSUSE-SU-2016:1292-1)	Vulnerability - level 4	Vuln
168857	OpenSUSE Security Update for libressl (openSUSE-SU-2016:1327-1)	Vulnerability - level 3	Vuln
168858	OpenSUSE Security Update for ntp (openSUSE-SU-2016:1329-1)	Vulnerability - level 4	Vuln
168861	OpenSUSE Security Update for mysql-community-server (openSUSE-SU-2016:1332-1)	Vulnerability - level 4	Vuln
168872	SUSE Enterprise Linux Security update for openssh (SUSE-SU-2016:1386-1)	Vulnerability - level 3	Vuln
168876	OpenSUSE Security Update for ntp (openSUSE-SU-2016:1423-1)	Vulnerability - level 3	Vuln
168886	OpenSUSE Security Update for openssh (openSUSE-SU-2016:1455-1)	Vulnerability - level 3	Vuln
168911	OpenSUSE Security Update for nodejs (openSUSE-SU-2016:1566-1)	Vulnerability - level 4	Vuln
168914	OpenSUSE Security Update for ntp (openSUSE-SU-2016:1583-1)	Vulnerability - level 4	Vuln
168925	OpenSUSE Security Update for ntp (openSUSE-SU-2016:1636-1)	Vulnerability - level 4	Vuln
168937	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2016:1584-1)	Vulnerability - level 4	Vuln
168940	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2016:1568-1)	Vulnerability - level 4	Vuln

168941	SUSE Enterprise Linux Security update for ntp (SUSE-SU-2016:1563-1)	Vulnerability - level 4	Vuln
168968	OpenSUSE Security Update for flash-player (openSUSE-SU-2016:1795-1)	Vulnerability - level 4	Vuln
168970	OpenSUSE Security Update for flash-player (openSUSE-SU-2016:1802-1)	Vulnerability - level 4	Vuln
168972	OpenSUSE Security Update for xerces-c (openSUSE-SU-2016:1808-1)	Vulnerability - level 3	Vuln
168975	SUSE Enterprise Linux Security update for Apache2 (SUSE-SU-2016:1818-1) (HTTPoxy)	Vulnerability - level 4	Vuln
168976	SUSE Enterprise Linux Security update for Apache2 (SUSE-SU-2016:1819-1) (HTTPoxy)	Vulnerability - level 4	Vuln
168979	OpenSUSE Security Update for apache2 (openSUSE-SU-2016:1824-1) (HTTPoxy)	Vulnerability - level 3	Vuln
168991	SUSE Enterprise Linux Security Update for flash-player (SUSE-SU-2016:1826-1)	Vulnerability - level 4	Vuln
168994	SUSE Enterprise Linux Security Update for php5 (SUSE-SU-2016:1842-1)	Vulnerability - level 3	Vuln
168997	SUSE Enterprise Linux Security Update for ntp (SUSE-SU-2016:1602-1)	Vulnerability - level 4	Vuln
169002	SUSE Enterprise Linux Security Update for mysql (SUSE-SU-2016:1618-1)	Vulnerability - level 3	Vuln
169013	SUSE Enterprise Linux Security Update for ntp (SUSE-SU-2016:1912-1)	Vulnerability - level 4	Vuln
169075	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2016:2090-1)	Vulnerability - level 3	Vuln
169077	SUSE Enterprise Linux Security Update for yast2-ntp-client (SUSE-SU-2016:2094-1)	Vulnerability - level 4	Vuln
169089	SUSE Enterprise Linux Security Update for xerces-c (SUSE-SU-2016:2154-1)	Vulnerability - level 3	Vuln
169091	OpenSUSE Security Update for php5 (openSUSE-SU-2016:1922-1)	Vulnerability - level 3	Vuln
169122	OpenSUSE Security Update for apache2-mod_fcgid (openSUSE-SU-2016:2115-1)	Vulnerability - level 3	Vuln
169137	SUSE Enterprise Linux Security Update for tomcat (SUSE-SU-2016:2188-1)	Vulnerability - level 3	Vuln
169148	SUSE Enterprise Linux Security Update for tomcat6 (SUSE-SU-2016:2229-1)	Vulnerability - level 3	Vuln
169160	SUSE Enterprise Linux Security Update for apache2-mod_nss (SUSE-SU-2016:2285-1)	Vulnerability - level 3	Vuln
169169	SUSE Enterprise Linux Security Update for apache2-mod_nss (SUSE-SU-2016:2329-1)	Vulnerability - level 3	Vuln
169170	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2016:2330-1)	Vulnerability - level 3	Vuln
169183	OpenSUSE Security Update for curl (openSUSE-SU-2016:2227-1)	Vulnerability - level 3	Vuln
169184	OpenSUSE Security Update for xerces-c (openSUSE-SU-2016:2232-1)	Vulnerability - level 3	Vuln
169186	OpenSUSE Security Update for tomcat (openSUSE-SU-2016:2252-1)	Vulnerability - level 3	Vuln
169189	OpenSUSE Security Update for libtcnative-1-0 (openSUSE-SU-2016:2267-1)	Vulnerability - level 3	Vuln
169197	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2016:2290-1)	Vulnerability - level 4	Vuln
169215	OpenSUSE Security Update for curl (openSUSE-SU-2016:2379-1)	Vulnerability - level 3	Vuln
169217	SUSE Enterprise Linux Security Update for libtcnative-1-0 (SUSE-SU-2016:2385-1)	Vulnerability - level 3	Vuln
169219	SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2016:2388-1)	Vulnerability - level 3	Vuln
169221	SUSE Enterprise Linux Security Update for openssl (SUSE-SU-2016:2394-1)	Vulnerability - level 4	Vuln

169232	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2016:2449-1)	Vulnerability - level 3	Vuln
169234	SUSE Enterprise Linux Security Update for openssl (SUSE-SU-2016:2458-1)	Vulnerability - level 4	Vuln
169237	SUSE Enterprise Linux Security Update for compat-openssl098 (SUSE-SU-2016:2468-1)	Vulnerability - level 4	Vuln
169266	OpenSUSE Security Update for nodejs (openSUSE-SU-2016:2496-1)	Vulnerability - level 4	Vuln
169277	OpenSUSE Security Update for compat-openssl098 (openSUSE-SU-2016:2537-1)	Vulnerability - level 4	Vuln
169330	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2016:2699-1)	Vulnerability - level 4	Vuln
169332	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2016:2714-1)	Vulnerability - level 4	Vuln
169343	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2016:2625-1)	Vulnerability - level 4	Vuln
169360	OpenSUSE Security Update for jasper (openSUSE-SU-2016:2722-1)	Vulnerability - level 3	Vuln
169365	OpenSUSE Security Update for jasper (openSUSE-SU-2016:2737-1)	Vulnerability - level 3	Vuln
169370	OpenSUSE Security Update for curl (openSUSE-SU-2016:2768-1)	Vulnerability - level 4	Vuln
169371	OpenSUSE Security Update for mysql-community-server (openSUSE-SU-2016:2769-1)	Vulnerability - level 4	Vuln
169376	OpenSUSE Security Update for mysql-community-server (openSUSE-SU-2016:2788-1)	Vulnerability - level 4	Vuln
169400	SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2016:2941-1)	Vulnerability - level 3	Vuln
169442	SUSE Enterprise Linux Security Update for ntp (SUSE-SU-2016:3193-1)	Vulnerability - level 3	Vuln
169443	SUSE Enterprise Linux Security Update for ntp (SUSE-SU-2016:3195-1)	Vulnerability - level 3	Vuln
169468	SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2016:3301-1)	Vulnerability - level 3	Vuln
169478	SUSE Enterprise Linux Security Update for freeradius-server (SUSE-SU-2017:0102-1)	Vulnerability - level 4	Vuln
169502	SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2017:0264-1)	Vulnerability - level 3	Vuln
169569	OpenSUSE Security Update for tiff (openSUSE-SU-2016:3035-1)	Vulnerability - level 4	Vuln
169588	OpenSUSE Security Update for php7 (openSUSE-SU-2016:3092-1)	Vulnerability - level 3	Vuln
169612	OpenSUSE Security Update for mcabber (openSUSE-SU-2016:3218-1)	Vulnerability - level 3	Vuln
169618	OpenSUSE Security Update for ntp (openSUSE-SU-2016:3280-1)	Vulnerability - level 3	Vuln
169640	OpenSUSE Security Update for tiff (openSUSE-SU-2017:0074-1)	Vulnerability - level 3	Vuln
169681	OpenSUSE Security Update for python3-sleekxmpp (openSUSE-SU-2017:0259-1)	Vulnerability - level 3	Vuln
169690	OpenSUSE Security Update for openssh (openSUSE-SU-2017:0344-1)	Vulnerability - level 3	Vuln
169711	SUSE Enterprise Linux Security Update for openssl (SUSE-SU-2017:0461-1)	Vulnerability - level 3	Vuln
169756	OpenSUSE Security Update for openssl (openSUSE-SU-2017:0487-1)	Vulnerability - level 3	Vuln
169778	SUSE Enterprise Linux Security Update for openssl (SUSE-SU-2017:0585-1)	Vulnerability - level 3	Vuln
169784	SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2017:0603-1)	Vulnerability - level 3	Vuln
169785	SUSE Enterprise Linux Security Update for compat-openssl098 (SUSE-SU-2017:0605-1)	Vulnerability - level 3	Vuln
169794	SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2017:0607-1)	Vulnerability - level 3	Vuln
169799	SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2017:0607-2)	Vulnerability - level 3	Vuln

169832	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2017:0864-1)	Vulnerability - level 4	Vuln
169833	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2017:0865-1)	Vulnerability - level 4	Vuln
169861	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2017:1043-1)	Vulnerability - level 3	Vuln
169863	SUSE Enterprise Linux Security Update for ntp (SUSE-SU-2017:1048-1)	Vulnerability - level 3	Vuln
169864	SUSE Enterprise Linux Security Update for ntp (SUSE-SU-2017:1052-1)	Vulnerability - level 3	Vuln
169872	SUSE Enterprise Linux Security Update for ruby2.1 (SUSE-SU-2017:1067-1)	Vulnerability - level 4	Vuln
169881	OpenSUSE Security Update for openssh (openSUSE-SU-2017:0674-1)	Vulnerability - level 3	Vuln
169901	OpenSUSE Security Update for pidgin (openSUSE-SU-2017:0892-1)	Vulnerability - level 3	Vuln
169910	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2017:0906-1)	Vulnerability - level 4	Vuln
169911	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2017:0907-1)	Vulnerability - level 4	Vuln
169915	OpenSUSE Security Update for pidgin (openSUSE-SU-2017:0925-1)	Vulnerability - level 3	Vuln
169925	OpenSUSE Security Update for pidgin (openSUSE-SU-2017:0973-1)	Vulnerability - level 4	Vuln
169979	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2017:1301-1)	Vulnerability - level 4	Vuln
170028	OpenSUSE Security Update for libressl (openSUSE-SU-2017:1211-1)	Vulnerability - level 3	Vuln
170029	OpenSUSE Security Update for libressl (openSUSE-SU-2017:1212-1)	Vulnerability - level 3	Vuln
170066	SUSE Enterprise Linux Security Update for jakarta-taglibs-standard (SUSE-SU-2017:1568-1)	Vulnerability - level 4	Vuln
170080	SUSE Enterprise Linux Security Update for openvpn (SUSE-SU-2017:1622-1)	Vulnerability - level 4	Vuln
170112	OpenSUSE Security Update for openvpn (openSUSE-SU-2017:1638-1)	Vulnerability - level 4	Vuln
170113	SUSE Enterprise Linux Security Update for tomcat6 (SUSE-SU-2017:1632-1)	Vulnerability - level 4	Vuln
170126	SUSE Enterprise Linux Security Update for jakarta-taglibs-standard (SUSE-SU-2017:1701-1)	Vulnerability - level 4	Vuln
170142	SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2017:1774-1)	Vulnerability - level 4	Vuln
170144	SUSE Enterprise Linux Security Update for freeradius-server (SUSE-SU-2017:1777-1)	Vulnerability - level 3	Vuln
170198	OpenSUSE Security Update for qemu (openSUSE-SU-2017:1872-1)	Vulnerability - level 4	Vuln
170243	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2017:2115-1)	Vulnerability - level 3	Vuln
170247	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2017:2141-1)	Vulnerability - level 2	Vuln
170254	SUSE Enterprise Linux Security Update for java-1_8_0-openjdk (SUSE-SU-2017:2175-1)	Vulnerability - level 4	Vuln
170256	SUSE Enterprise Linux Security Update for subversion (SUSE-SU-2017:2200-1)	Vulnerability - level 4	Vuln
170268	SUSE Enterprise Linux Security Update for mercurial (SUSE-SU-2017:2250-1)	Vulnerability - level 3	Vuln
170269	SUSE Enterprise Linux Security Update for mercurial (SUSE-SU-2017:2251-1)	Vulnerability - level 3	Vuln
170271	SUSE Enterprise Linux Security Update for java-1_8_0-ibm (SUSE-SU-2017:2263-1)	Vulnerability - level 4	Vuln
170276	SUSE Enterprise Linux Security Update for java-1_7_1-ibm (SUSE-SU-2017:2280-1)	Vulnerability - level 4	Vuln

170277	SUSE Enterprise Linux Security Update for java-1_7_1-ibm (SUSE-SU-2017:2281-1)	Vulnerability - level 4	Vuln
170301	OpenSUSE Security Update for libxml2 (openSUSE-SU-2017:2190-1)	Vulnerability - level 2	Vuln
170324	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2017:2312-1)	Vulnerability - level 3	Vuln
170424	SUSE Enterprise Linux Security Update for wpa_supplicant (SUSE-SU-2017:2745-1) (KRACK Attack)	Vulnerability - level 4	Vuln
170428	SUSE Enterprise Linux Security Update for wpa_supplicant (SUSE-SU-2017:2752-1) (KRACK Attack)	Vulnerability - level 4	Vuln
170431	SUSE Enterprise Linux Security Update for openvpn (SUSE-SU-2017:2838-1)	Vulnerability - level 4	Vuln
170433	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2017:2847-1)	Vulnerability - level 4	Vuln
170440	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2017:2869-1)	Vulnerability - level 4	Vuln
170455	OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2017:2755-1)	Vulnerability - level 4	Vuln
170469	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2017:2846-1)	Vulnerability - level 4	Vuln
170483	SUSE Enterprise Linux Security Update for kvm (SUSE-SU-2017:2963-1)	Vulnerability - level 4	Vuln
170502	SUSE Enterprise Linux Security Update for kernel-firmware (SUSE-SU-2017:3106-1)	Vulnerability - level 4	Vuln
170508	SUSE Enterprise Linux Security Update for openssl (SUSE-SU-2017:3169-1)	Vulnerability - level 3	Vuln
170519	SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2017:3230-1)	Vulnerability - level 3	Vuln
170527	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2017:3265-1)	Vulnerability - level 4	Vuln
170540	OpenSUSE Security Update for hostapd (openSUSE-SU-2017:2896-1)	Vulnerability - level 4	Vuln
170544	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2017:2905-1)	Vulnerability - level 4	Vuln
170554	OpenSUSE Security Update for ansible (openSUSE-SU-2017:2976-1)	Vulnerability - level 3	Vuln
170580	OpenSUSE Security Update for kernel-firmware (openSUSE-SU-2017:3144-1)	Vulnerability - level 4	Vuln
170582	OpenSUSE Security Update for openssl (openSUSE-SU-2017:3192-1)	Vulnerability - level 3	Vuln
170599	OpenSUSE Security Update for openssh (openSUSE-SU-2017:3243-1)	Vulnerability - level 3	Vuln
170609	SUSE Enterprise Linux Security Update for openssl (SUSE-SU-2017:3343-1)	Vulnerability - level 4	Vuln
170641	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL) (openSUSE-SU-2017:3345-1)	Vulnerability - level 4	Vuln
170665	OpenSUSE Security Update for nodejs4 (openSUSE-SU-2018:0029-1)	Vulnerability - level 3	Vuln
170667	OpenSUSE Security Update for java-1_7_0-openjdk (openSUSE-SU-2018:0042-1)	Vulnerability - level 4	Vuln
170714	SUSE Enterprise Linux Security Update for webkit2gtk3 (SUSE-SU-2018:0219-1)	Vulnerability - level 4	Vuln
170765	SUSE Enterprise Linux Security Update for quagga (SUSE-SU-2018:0456-1)	Vulnerability - level 4	Vuln
170766	SUSE Enterprise Linux Security Update for quagga (SUSE-SU-2018:0457-1)	Vulnerability - level 4	Vuln
170817	OpenSUSE Security Update for mysql-community-server (openSUSE-SU-2018:0223-1)	Vulnerability - level 4	Vuln

170828	OpenSUSE Security Update for nodejs6 (openSUSE-SU-2018:0315-1)	Vulnerability - level 3	Vuln
170835	OpenSUSE Security Update for webkit2gtk3 (openSUSE-SU-2018:0326-1)	Vulnerability - level 4	Vuln
170864	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer Steam (OpenSSLsteam) (openSUSE-SU-2018:0458-1)	Vulnerability - level 4	Vuln
170871	OpenSUSE Security Update for quagga (openSUSE-SU-2018:0473-1)	Vulnerability - level 4	Vuln
171101	OpenSUSE Security Update for virtualbox (openSUSE-SU-2018:1057-1)	Vulnerability - level 4	Vuln
171224	SUSE Enterprise Linux Security Update for nagios-nrpe (SUSE-SU-2018:1768-1)	Vulnerability - level 3	Vuln
171270	SUSE Enterprise Linux Security Update for openssl (SUSE-SU-2018:1887-1)	Vulnerability - level 3	Vuln
171274	SUSE Enterprise Linux Security Update for (SUSE-SU-2018:1935-1)	Vulnerability - level 4	Vuln
171347	OpenSUSE Security Update for ucode-intel (openSUSE-SU-2018:1904-1)	Vulnerability - level 4	Vuln
171349	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL) (openSUSE-SU-2018:1906-1)	Vulnerability - level 3	Vuln
171378	SUSE Enterprise Linux Security Update for microcode_ctl (SUSE-SU-2018:2076-1)	Vulnerability - level 4	Vuln
171389	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2018:2207-1)	Vulnerability - level 3	Vuln
171390	SUSE Enterprise Linux Security update for unzip (CVE-2005-2475)	Vulnerability - level 3	Vuln
171393	SUSE Enterprise Linux Security Update for pidgin (SUSE-SU-2018:2235-1)	Vulnerability - level 3	Vuln
171394	SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2018:2275-1)	Vulnerability - level 3	Vuln
171418	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2018:2242-1)	Vulnerability - level 4	Vuln
171443	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2018:2328-1)	Vulnerability - level 4	Vuln
171445	SUSE Enterprise Linux Security Update for (SUSE-SU-2018:2331-1)	Vulnerability - level 4	Vuln
171448	SUSE Enterprise Linux Security Update for (SUSE-SU-2018:2335-1)	Vulnerability - level 4	Vuln
171450	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2018:2374-1)	Vulnerability - level 4	Vuln
171485	Software and Systems Development (SUSE) Enterprise Linux Security Update for Compat-Open Secure Sockets Layer (compat-OpenSSL098) (SUSE-SU-2018:2683-1)	Vulnerability - level 3	Vuln
171487	SUSE Enterprise Linux Security Update for tomcat (SUSE-SU-2018:2699-1)	Vulnerability - level 3	Vuln
171488	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2018:2715-1)	Vulnerability - level 3	Vuln
171489	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2018:2717-1)	Vulnerability - level 3	Vuln
171503	SUSE Enterprise Linux Security Update for java-1_8_0-ibm (SUSE-SU-2018:2839-1)	Vulnerability - level 3	Vuln
171520	OpenSUSE Security Update for ucode-intel (openSUSE-SU-2018:2399-1)	Vulnerability - level 4	Vuln
171523	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2018:2404-1)	Vulnerability - level 4	Vuln
171562	OpenSUSE Security Update for nodejs4 (openSUSE-SU-2018:2667-1)	Vulnerability - level 3	Vuln
171566	Open Software and Systems Development (OpenSUSE) Security Update for Compat-Open Secure Sockets Layer (compat-OpenSSL098) (openSUSE-SU-2018:2695-1)	Vulnerability - level 3	Vuln

171571	OpenSUSE Security Update for curl (openSUSE-SU-2018:2731-1)	Vulnerability - level 3	Vuln
171573	OpenSUSE Security Update for curl (openSUSE-SU-2018:2736-1)	Vulnerability - level 3	Vuln
171575	OpenSUSE Security Update for tomcat (openSUSE-SU-2018:2740-1)	Vulnerability - level 3	Vuln
171586	OpenSUSE Security Update for nodejs6 (openSUSE-SU-2018:2816-1)	Vulnerability - level 3	Vuln
171609	OpenSUSE Security Update for nodejs8 (openSUSE-SU-2018:2855-1)	Vulnerability - level 3	Vuln
171656	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (openSUSE-SU-2018:3013-1)	Vulnerability - level 3	Vuln
171658	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (openSUSE-SU-2018:3015-1)	Vulnerability - level 3	Vuln
171664	SUSE Enterprise Linux Security Update for Xerces-c (SUSE-SU-2018:3277-1)	Vulnerability - level 3	Vuln
171702	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2018:3608-1)	Vulnerability - level 3	Vuln
171707	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2018:3681-1)	Vulnerability - level 3	Vuln
171789	SUSE Enterprise Linux Security Update for MozillaFirefox, mozilla-nspr and mozilla-nss (SUSE-SU-2018:4236-1)	Vulnerability - level 4	Vuln
171808	OpenSUSE Security Update for tomcat (openSUSE-SU-2018:3054-1)	Vulnerability - level 3	Vuln
171837	SUSE Enterprise Linux Security Update for LibVNCServer (SUSE-SU-2019:0060-1)	Vulnerability - level 4	Vuln
171840	SUSE Enterprise Linux Security Update for LibVNCServer (SUSE-SU-2019:13927-1)	Vulnerability - level 4	Vuln
171878	OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2018:3539-1)	Vulnerability - level 3	Vuln
171887	OpenSUSE Security Update for curl (openSUSE-SU-2018:3699-1)	Vulnerability - level 3	Vuln
171890	OpenSUSE Security Update for curl (openSUSE-SU-2018:3706-1)	Vulnerability - level 3	Vuln
171944	OpenSUSE Security Update for mozilla-nss (openSUSE-SU-2018:4117-1)	Vulnerability - level 3	Vuln
171975	OpenSUSE Security Update for mozilla-nspr and mozilla-nss (openSUSE-SU-2018:4283-1)	Vulnerability - level 3	Vuln
171990	OpenSUSE Security Update for LibVNCServer (openSUSE-SU-2019:0045-1)	Vulnerability - level 4	Vuln
171996	OpenSUSE Security Update for LibVNCServer (openSUSE-SU-2019:0053-1)	Vulnerability - level 4	Vuln
172073	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2019:0339-1)	Vulnerability - level 4	Vuln
172095	OpenSUSE Security Update for mozilla-nss (openSUSE-SU-2019:0183-1)	Vulnerability - level 4	Vuln
172278	SUSE Enterprise Linux Security Update for python3 (SUSE-SU-2019:0961-1)	Vulnerability - level 4	Vuln
172291	SUSE Enterprise Linux Security Update for wpa_supplicant (SUSE-SU-2019:1088-1)	Vulnerability - level 3	Vuln
172341	OpenSUSE Security Update for python (openSUSE-SU-2019:1273-1)	Vulnerability - level 4	Vuln
172345	OpenSUSE Security Update for python3 (openSUSE-SU-2019:1282-1)	Vulnerability - level 4	Vuln
172368	OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2019:1345-1)	Vulnerability - level 3	Vuln
172378	OpenSUSE Security Update for python3 (openSUSE-SU-2019:1371-1)	Vulnerability - level 4	Vuln
172443	SUSE Enterprise Linux Security Update for python (SUSE-SU-2019:1439-1)	Vulnerability - level 4	Vuln

172536	SUSE Enterprise Linux Security Update for subversion (SUSE-SU-2019:2032-1)	Vulnerability - level 4	Vuln
172540	SUSE Enterprise Linux Security Update for python3 (SUSE-SU-2019:2053-1)	Vulnerability - level 4	Vuln
172548	SUSE Enterprise Linux Security Update for python (SUSE-SU-2019:2091-1)	Vulnerability - level 4	Vuln
172588	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (SUSE-SU-2019:2504-1)	Vulnerability - level 3	Vuln
172594	Software and Systems Development (SUSE) Enterprise Linux Security Update for Compat-Open Secure Sockets Layer (compat-OpenSSL098) (SUSE-SU-2019:2558-1)	Vulnerability - level 3	Vuln
172616	OpenSUSE Security Update for python (openSUSE-SU-2019:1580-1)	Vulnerability - level 4	Vuln
172641	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (openSUSE-SU-2019:2268-1)	Vulnerability - level 3	Vuln
172644	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (openSUSE-SU-2019:2269-1)	Vulnerability - level 3	Vuln
172746	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (openSUSE-SU-2019:2158-1)	Vulnerability - level 3	Vuln
172761	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (openSUSE-SU-2019:2189-1)	Vulnerability - level 3	Vuln
172829	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 32 for SLE 12 SP2) (SUSE-SU-2019:2601-1)	Vulnerability - level 4	Vuln
172838	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 33 for SLE 12 SP1) (SUSE-SU-2019:2821-1)	Vulnerability - level 4	Vuln
172929	SUSE Enterprise Linux Security Update for MozillaFirefox (SUSE-SU-2019:3347-1)	Vulnerability - level 3	Vuln
172970	SUSE Enterprise Linux Security Update for mozilla-nspr, mozilla-nss (SUSE-SU-2020:0088-1)	Vulnerability - level 3	Vuln
172973	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2020:0099-1)	Vulnerability - level 3	Vuln
172994	SUSE Enterprise Linux Security Update for python36 (SUSE-SU-2020:0302-1)	Vulnerability - level 4	Vuln
173025	OpenSUSE Security Update for MozillaThunderbird (openSUSE-SU-2020:0003-1)	Vulnerability - level 4	Vuln
173026	OpenSUSE Security Update for MozillaFirefox (openSUSE-SU-2020:0002-1)	Vulnerability - level 4	Vuln
173028	OpenSUSE Security Update for mozilla-nspr, mozilla-nss (openSUSE-SU-2020:0008-1)	Vulnerability - level 3	Vuln
173049	OpenSUSE Security Update for python3 (openSUSE-SU-2020:0086-1)	Vulnerability - level 4	Vuln
173133	OpenSUSE Security Update for chromium (openSUSE-SU-2020:0189-1)	Vulnerability - level 4	Vuln
173189	SUSE Enterprise Linux Security Update for vino (SUSE-SU-2020:0955-1)	Vulnerability - level 3	Vuln
173216	OpenSUSE Security Update for python-Django (openSUSE-SU-2019:1839-1)	Vulnerability - level 3	Vuln
173224	OpenSUSE Security Update for python (openSUSE-SU-2019:1906-1)	Vulnerability - level 4	Vuln
173271	SUSE Enterprise Linux Security Update for LibVNCServer (SUSE-SU-2020:1165-1)	Vulnerability - level 4	Vuln
173286	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1255-1)	Vulnerability - level 4	Vuln

173288	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1275-1)	Vulnerability - level 4	Vuln
173305	OpenSUSE Security Update for LibVNCServer (openSUSE-SU-2020:0624-1)	Vulnerability - level 4	Vuln
173363	OpenSUSE Security Update for MozillaFirefox (openSUSE-SU-2019:1758-1)	Vulnerability - level 4	Vuln
173431	OpenSUSE Security Update for subversion (openSUSE-SU-2019:1910-1)	Vulnerability - level 4	Vuln
173456	OpenSUSE Security Update for proftpd (openSUSE-SU-2020:0273-1)	Vulnerability - level 3	Vuln
173534	SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2020:1568-1)	Vulnerability - level 5	Vuln
173539	SUSE Enterprise Linux Security Update for nodejs8 (SUSE-SU-2020:1576-1)	Vulnerability - level 5	Vuln
173541	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1587-1)	Vulnerability - level 4	Vuln
173543	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:1595-1)	Vulnerability - level 3	Vuln
173544	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1596-1)	Vulnerability - level 4	Vuln
173545	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:1600-1)	Vulnerability - level 3	Vuln
173546	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1597-1)	Vulnerability - level 4	Vuln
173547	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:1601-1)	Vulnerability - level 3	Vuln
173548	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1603-1)	Vulnerability - level 4	Vuln
173549	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1602-1)	Vulnerability - level 4	Vuln
173550	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1605-1)	Vulnerability - level 4	Vuln
173567	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:0801-1)	Vulnerability - level 4	Vuln
173569	OpenSUSE Security Update for nodejs8 (openSUSE-SU-2020:0802-1)	Vulnerability - level 5	Vuln
173570	OpenSUSE Security Update for xen (openSUSE-SU-2020:0818-1)	Vulnerability - level 4	Vuln
173573	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2020:1630-1)	Vulnerability - level 4	Vuln
173574	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2020:1634-1)	Vulnerability - level 4	Vuln
173575	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2020:1633-1)	Vulnerability - level 4	Vuln
173576	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2020:1632-1)	Vulnerability - level 3	Vuln
173582	OpenSUSE Security Update for libxml2 (openSUSE-SU-2020:0781-1)	Vulnerability - level 3	Vuln
173585	OpenSUSE Security Update for ucode-intel (openSUSE-SU-2020:0791-1)	Vulnerability - level 3	Vuln
173593	OpenSUSE Security Update for libxml2 (openSUSE-SU-2020:0681-1)	Vulnerability - level 3	Vuln
173609	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1663-1)	Vulnerability - level 4	Vuln
173712	OpenSUSE Security Update for LibVNCServer (openSUSE-SU-2020:0960-1)	Vulnerability - level 4	Vuln
173716	OpenSUSE Security Update for xen (openSUSE-SU-2020:0965-1)	Vulnerability - level 4	Vuln
173719	OpenSUSE Security Update for LibVNCServer (openSUSE-SU-2020:0978-1)	Vulnerability - level 4	Vuln
173721	OpenSUSE Security Update for xen (openSUSE-SU-2020:0985-1)	Vulnerability - level 4	Vuln

173722	OpenSUSE Security Update for LibVNCServer (openSUSE-SU-2020:0988-1)	Vulnerability - level 4	Vuln
173740	OpenSUSE Security Update for LibVNCServer (openSUSE-SU-2020:1025-1)	Vulnerability - level 4	Vuln
173755	OpenSUSE Security Update for LibVNCServer (openSUSE-SU-2020:1056-1)	Vulnerability - level 4	Vuln
173758	OpenSUSE Security Update for vino (openSUSE-SU-2020:1071-1)	Vulnerability - level 3	Vuln
173768	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2020:2079-1)	Vulnerability - level 4	Vuln
173769	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2020:2078-1)	Vulnerability - level 4	Vuln
173770	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2020:2076-1)	Vulnerability - level 4	Vuln
173771	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2020:2073-1)	Vulnerability - level 4	Vuln
173784	OpenSUSE Security Update for grub2 (openSUSE-SU-2020:1168-1)	Vulnerability - level 2	Vuln
173785	OpenSUSE Security Update for grub2 (openSUSE-SU-2020:1169-1)	Vulnerability - level 2	Vuln
173858	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2020:1887-1)	Vulnerability - level 4	Vuln
173888	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2020:2078-1)	Vulnerability - level 2	Vuln
173905	SUSE Enterprise Linux Security Update for LibVNCServer (SUSE-SU-2020:2167-1)	Vulnerability - level 4	Vuln
173933	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2020:2304-1)	Vulnerability - level 4	Vuln
173934	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2020:2308-1)	Vulnerability - level 4	Vuln
173935	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2020:2303-1)	Vulnerability - level 4	Vuln
173937	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2020:2305-1)	Vulnerability - level 4	Vuln
173970	OpenSUSE Security Update for grub2 (openSUSE-SU-2020:1280-1)	Vulnerability - level 2	Vuln
173972	OpenSUSE Security Update for grub2 (openSUSE-SU-2020:1282-1)	Vulnerability - level 4	Vuln
174027	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2020:2609-1)	Vulnerability - level 3	Vuln
174053	Software and Systems Development (SUSE) Enterprise Linux Security Update for Compat-Open Secure Sockets Layer (compat-OpenSSL098) (SUSE-SU-2020:2634-1)	Vulnerability - level 2	Vuln
174094	OpenSUSE Security Update for nodejs12 (openSUSE-SU-2020:1616-1)	Vulnerability - level 4	Vuln
174123	SUSE Enterprise Linux Security Update for nodejs8 (SUSE-SU-2020:2800-1)	Vulnerability - level 4	Vuln
174126	SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2020:2813-1)	Vulnerability - level 4	Vuln
174127	SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2020:2812-1)	Vulnerability - level 4	Vuln
174129	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2020:2822-1)	Vulnerability - level 4	Vuln
174130	SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2020:2823-1)	Vulnerability - level 4	Vuln
174132	SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2020:2829-1)	Vulnerability - level 4	Vuln
174146	OpenSUSE Security Update for nodejs10 (openSUSE-SU-2020:1660-1)	Vulnerability - level 4	Vuln
174331	SUSE Enterprise Linux Security Update for u-boot (SUSE-SU-2020:3255-1)	Vulnerability - level 4	Vuln
174336	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:3276-1)	Vulnerability - level 1	Vuln

174337	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3273-1)	Vulnerability - level 1	Vuln
174338	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:3275-1)	Vulnerability - level 1	Vuln
174339	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3272-1)	Vulnerability - level 2	Vuln
174340	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:3274-1)	Vulnerability - level 1	Vuln
174341	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:3271-1)	Vulnerability - level 1	Vuln
174343	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:3279-1)	Vulnerability - level 1	Vuln
174344	SUSE Enterprise Linux Security Update for u-boot (SUSE-SU-2020:3282-1)	Vulnerability - level 4	Vuln
174345	SUSE Enterprise Linux Security Update for u-boot (SUSE-SU-2020:3283-1)	Vulnerability - level 4	Vuln
174346	SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2020:3315-1)	Vulnerability - level 4	Vuln
174347	SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2020:3313-1)	Vulnerability - level 4	Vuln
174348	SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2020:3314-1)	Vulnerability - level 2	Vuln
174366	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:3372-1)	Vulnerability - level 3	Vuln
174369	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:3373-1)	Vulnerability - level 3	Vuln
174370	SUSE Enterprise Linux Security Update for wpa_supplicant (SUSE-SU-2020:3380-1)	Vulnerability - level 3	Vuln
174377	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:3374-1)	Vulnerability - level 3	Vuln
174386	SUSE Enterprise Linux Security Update for wpa_supplicant (SUSE-SU-2020:3424-1)	Vulnerability - level 3	Vuln
174388	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:3457-1)	Vulnerability - level 3	Vuln
174400	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3501-1)	Vulnerability - level 4	Vuln
174401	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3503-1)	Vulnerability - level 4	Vuln
174402	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3507-1)	Vulnerability - level 4	Vuln
174404	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2020:3514-1)	Vulnerability - level 3	Vuln
174406	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3532-1)	Vulnerability - level 4	Vuln
174407	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3544-1)	Vulnerability - level 4	Vuln
174444	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 18 for SLE 15 SP1) (SUSE-SU-2020:3690-1)	Vulnerability - level 4	Vuln
174447	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 7 for SLE 12 SP5) (SUSE-SU-2020:3670-1)	Vulnerability - level 4	Vuln
174448	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 32 for SLE 12 SP3) (SUSE-SU-2020:3651-1)	Vulnerability - level 4	Vuln
174450	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3715-1)	Vulnerability - level 4	Vuln
174454	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2020:3720-1)	Vulnerability - level 4	Vuln

174456	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2020:3721-1)	Vulnerability - level 4	Vuln
174457	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2020:3722-1)	Vulnerability - level 4	Vuln
174459	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2020:3733-1)	Vulnerability - level 3	Vuln
174461	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (SUSE-SU-2020:3732-1)	Vulnerability - level 4	Vuln
174462	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2020:3735-1)	Vulnerability - level 3	Vuln
174467	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2020:3740-1)	Vulnerability - level 4	Vuln
174468	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2020:3739-1)	Vulnerability - level 3	Vuln
174469	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3748-1)	Vulnerability - level 4	Vuln
174472	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2020:3763-1)	Vulnerability - level 4	Vuln
174519	SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2021:0068-1)	Vulnerability - level 3	Vuln
174520	SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2021:0062-1)	Vulnerability - level 3	Vuln
174521	SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2021:0060-1)	Vulnerability - level 3	Vuln
174526	SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2021:0082-1)	Vulnerability - level 3	Vuln
174540	SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2021:0128-1)	Vulnerability - level 3	Vuln
174544	SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2021:0129-1)	Vulnerability - level 3	Vuln
174547	SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2021:0142-1)	Vulnerability - level 3	Vuln
174552	SUSE Enterprise Linux Security Update for dnsmasq (SUSE-SU-2021:0163-1)	Vulnerability - level 4	Vuln
174553	SUSE Enterprise Linux Security Update for dnsmasq (SUSE-SU-2021:0166-1)	Vulnerability - level 4	Vuln
174554	SUSE Enterprise Linux Security Update for dnsmasq (SUSE-SU-2021:0162-1)	Vulnerability - level 4	Vuln
174581	SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2021:0258-1)	Vulnerability - level 4	Vuln
174584	SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2021:0276-1)	Vulnerability - level 4	Vuln
174585	SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2021:0284-1)	Vulnerability - level 4	Vuln
174588	SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2021:0298-1)	Vulnerability - level 4	Vuln
174589	SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2021:0300-1)	Vulnerability - level 4	Vuln
174591	SUSE Enterprise Linux Security Update for openvswitch (SUSE-SU-2021:0297-1)	Vulnerability - level 4	Vuln
174636	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:0507-1)	Vulnerability - level 4	Vuln
174637	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:0504-1)	Vulnerability - level 4	Vuln

174638	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:0503-1)	Vulnerability - level 4	Vuln
174670	SUSE Enterprise Linux Security Update for nodejs14 (SUSE-SU-2021:0650-1)	Vulnerability - level 4	Vuln
174671	SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2021:0651-1)	Vulnerability - level 4	Vuln
174673	SUSE Enterprise Linux Security Update for nodejs14 (SUSE-SU-2021:0648-1)	Vulnerability - level 4	Vuln
174674	SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2021:0649-1)	Vulnerability - level 4	Vuln
174683	SUSE Enterprise Linux Security Update for open-iscsi (SUSE-SU-2021:0663-1)	Vulnerability - level 4	Vuln
174687	SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2021:0673-1)	Vulnerability - level 4	Vuln
174688	SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2021:0674-1)	Vulnerability - level 4	Vuln
174689	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2021:0685-1)	Vulnerability - level 4	Vuln
174693	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2021:0681-1)	Vulnerability - level 4	Vuln
174694	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2021:0683-1)	Vulnerability - level 4	Vuln
174695	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2021:0682-1)	Vulnerability - level 4	Vuln
174696	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2021:0679-1)	Vulnerability - level 4	Vuln
174697	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2021:0684-1)	Vulnerability - level 4	Vuln
174699	SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2021:0693-1)	Vulnerability - level 3	Vuln
174722	SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2020:3717-1)	Vulnerability - level 3	Vuln
174739	SUSE Enterprise Linux Security update for openvswitch (SUSE-SU-2021:0277-1)	Vulnerability - level 4	Vuln
174780	SUSE Enterprise Linux Security update for openldap2 (SUSE-SU-2021:0692-1)	Vulnerability - level 3	Vuln
174783	SUSE Enterprise Linux Security update for openldap2 (SUSE-SU-2021:0723-1)	Vulnerability - level 3	Vuln
174784	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (SUSE-SU-2021:0725-1)	Vulnerability - level 2	Vuln
174785	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2021:0753-1)	Vulnerability - level 2	Vuln
174786	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2021:0754-1)	Vulnerability - level 2	Vuln
174787	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2021:0752-1)	Vulnerability - level 2	Vuln
174788	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2021:0755-1)	Vulnerability - level 2	Vuln
174789	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (SUSE-SU-2021:0769-1)	Vulnerability - level 2	Vuln
174794	Software and Systems Development (SUSE) Enterprise Linux Security Update for Compat-Open Secure Sockets Layer (compat-OpenSSL098) (SUSE-SU-2021:0793-1)	Vulnerability - level 2	Vuln

174830	SUSE Enterprise Linux Security update for nghttp2 (SUSE-SU-2021:0931-1)	Vulnerability - level 3	Vuln
174839	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2021:0939-1)	Vulnerability - level 2	Vuln
174844	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2021:0954-1)	Vulnerability - level 5	Vuln
174892	SUSE Enterprise Linux Security Update for open-iscsi (SUSE-SU-2021:1164-1)	Vulnerability - level 3	Vuln
174904	SUSE Enterprise Linux Security Update for nghttp2 (SUSE-SU-2021:0932-1)	Vulnerability - level 3	Vuln
174977	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:1469-1)	Vulnerability - level 4	Vuln
174978	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:1471-1)	Vulnerability - level 4	Vuln
174979	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:1468-1)	Vulnerability - level 4	Vuln
174983	SUSE Enterprise Linux Security Update for sca-patterns-sle11 (SUSE-SU-2021:1497-1)	Vulnerability - level 4	Vuln
174991	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2021:1524-1)	Vulnerability - level 3	Vuln
175004	Debian Security Update for Linux (DSA-1929)	Vulnerability - level 4	Vuln
175005	Debian Security Update for Linux (DSA-1928)	Vulnerability - level 4	Vuln
175007	Debian Security Update for Typo3 (DSA-1926)	Vulnerability - level 4	Vuln
175015	Debian Security Update for Libgd2 (DSA-1936)	Vulnerability - level 4	Vuln
175020	Debian Security Update for Poppler (DSA-1941)	Vulnerability - level 4	Vuln
175032	Debian Security Update for Asterisk (DSA-1952)	Vulnerability - level 4	Vuln
175039	Debian Security Update for Ganeti (DSA-1959)	Vulnerability - level 4	Vuln
175041	Debian Security Update for BIND9 (DSA-1961)	Vulnerability - level 4	Vuln
175075	Debian Security Update for OpenOffice.org (DSA-1995)	Vulnerability - level 3	Vuln
175076	Debian Security Update for Linux-2.6 (DSA-1996)	Vulnerability - level 3	Vuln
175078	Debian Security Update for Xulrunner (DSA-1999)	Vulnerability - level 4	Vuln
175082	Debian Security Update for Linux 2.6 (DSA-2003)	Vulnerability - level 4	Vuln
175083	Debian Security Update for Samba (DSA-2004)	Vulnerability - level 3	Vuln
175085	Debian Security Update for Linux-2.6.24 (DSA-2005)	Vulnerability - level 4	Vuln
175090	Debian Security Update for Linux 2.6 (DSA-2012)	Vulnerability - level 3	Vuln
175101	Debian Security Update for Curl (DSA-2023)	Vulnerability - level 3	Vuln
175106	Debian Security Update for Xulrunner (DSA-2027)	Vulnerability - level 3	Vuln
175109	Debian Security Update for Krb5 (DSA-2031)	Vulnerability - level 3	Vuln
175115	Debian Security Update for KDM (kdebase) (DSA-2037)	Vulnerability - level 3	Vuln
175118	Debian Security Update for SquidGuard (DSA-2040)	Vulnerability - level 3	Vuln
175124	Debian Security Update for phpGroupWare (DSA-2046)	Vulnerability - level 3	Vuln
175125	Debian Security Update for Aria2 (DSA-2047)	Vulnerability - level 3	Vuln
175130	Debian Security Update for Krb5 (DSA-2052)	Vulnerability - level 3	Vuln
175131	Debian Security Update for Linux-2.6 (DSA-2053)	Vulnerability - level 3	Vuln
175145	Debian Security Update for Libpam-krb5 (DSA-1721)	Vulnerability - level 3	Vuln
175146	Debian Security Update for Libpam-heimdal (DSA-1722)	Vulnerability - level 3	Vuln
175165	Debian Security Update for Libsndfile (DSA-1742)	Vulnerability - level 3	Vuln
175166	Debian Security Update for Libtk-img (DSA-1743)	Vulnerability - level 3	Vuln
175184	Debian Security Update for Strongswan (DSA-1759)	Vulnerability - level 3	Vuln
175185	Debian Security Update for Openswan (DSA-1760)	Vulnerability - level 3	Vuln
175191	Debian Security Update for Krb5 (DSA-1766)	Vulnerability - level 3	Vuln
175203	Debian Security Update for Xterm (DSA-1694)	Vulnerability - level 3	Vuln
175205	Debian Security Update for Iceape (DSA-1697)	Vulnerability - level 3	Vuln
175226	Debian Security Update for Apache2 (DSA-2298)	Vulnerability - level 3	Vuln
175241	Debian Security Update for OpenOffice.org (DSA-2473)	Vulnerability - level 3	Vuln
175248	Debian Security Update for openssl (DSA-2833-1)	Vulnerability - level 3	Vuln
175251	Debian Security Update for devscripts (DSA-2836-1)	Vulnerability - level 2	Vuln

175252	Debian Security Update for openssl (DSA-2837-1)	Vulnerability - level 4	Vuln
175274	Debian Security Update for libspring-java (DSA-2857-1)	Vulnerability - level 3	Vuln
175290	Debian Security Update for ntp (DSA 3154-1)	Vulnerability - level 4	Vuln
175293	Debian Security Update for ntp (DSA 3154-2)	Vulnerability - level 3	Vuln
175324	Debian Security Update for icu (DSA 3187-1)	Vulnerability - level 4	Vuln
175334	Debian Security Update for openssl (DSA 3197-1)	Vulnerability - level 4	Vuln
175342	Debian Security Update for openssl (DSA 3197-2)	Vulnerability - level 4	Vuln
175363	Debian Security Update for ntp (DSA 3223-1)	Vulnerability - level 3	Vuln
175371	Debian Security Update for subversion (DSA 3231-1)	Vulnerability - level 3	Vuln
175373	Debian Security Update for wpa (DSA 3233-1)	Vulnerability - level 3	Vuln
175434	Debian Security Update for openssl (DSA 3287-1)	Vulnerability - level 3	Vuln
175454	Debian Security Update for iceweasel (DSA 3300-1)	Vulnerability - level 3	Vuln
175462	Debian Security Update for pdns (DSA 3306-1)	Vulnerability - level 3	Vuln
175466	Debian Security Update for chromium-browser (DSA 3315-1)	Vulnerability - level 3	Vuln
175468	Debian Security Update for openjdk-7 (DSA 3316-1)	Vulnerability - level 3	Vuln
175475	Debian Security Update for icedove (DSA 3324-1)	Vulnerability - level 3	Vuln
175494	Debian Security Update for openjdk-6 (DSA 3339-1)	Vulnerability - level 3	Vuln
175544	Debian Security Update for ntp (DSA 3388-1)	Vulnerability - level 3	Vuln
175548	Debian Security Update for freeimage (DSA 3392-1)	Vulnerability - level 3	Vuln
175576	Debian Security Update for openssl (DSA 3413-1)	Vulnerability - level 3	Vuln
175599	Debian Security Update for tomcat7 (DSA 3447-1)	Vulnerability - level 3	Vuln
175645	Debian Security Update for xerces-c (DSA 3493-1)	Vulnerability - level 3	Vuln
175646	Debian Security Update for gajim (DSA 3492-1)	Vulnerability - level 3	Vuln
175654	Debian Security Update for openssl (DSA 3500-1)	Vulnerability - level 3	Vuln
175685	Debian Security Update for tomcat6 (DSA 3530-1)	Vulnerability - level 3	Vuln
175720	Debian Security Update for openssl (DSA 3566-1)	Vulnerability - level 3	Vuln
175721	Debian Security Update for openssh (DSA 3550-1)	Vulnerability - level 3	Vuln
175766	Debian Security Update for libpdfbox-java (DSA 3606-1)	Vulnerability - level 3	Vuln
175775	Debian Security Update for linux (DSA 3607-1)	Vulnerability - level 3	Vuln
175776	Debian Security Update for tomcat8 (DSA 3609-1)	Vulnerability - level 3	Vuln
175777	Debian Security Update for xerces-c (DSA 3610-1)	Vulnerability - level 3	Vuln
175789	Debian Security Update for apache2 (DSA 3623-1) (HTTPoxy)	Vulnerability - level 3	Vuln
175796	Debian Security Update for php5 (DSA 3631-1) (HTTPoxy)	Vulnerability - level 3	Vuln
175799	Debian Security Update for ntp (DSA 3629-1)	Vulnerability - level 3	Vuln
175804	Debian Security Update for curl (DSA 3638-1)	Vulnerability - level 3	Vuln
175840	Debian Security Update for openssl (DSA 3673-1)	Vulnerability - level 3	Vuln
175843	Debian Security Update for openssl (DSA 3673-2)	Vulnerability - level 3	Vuln
175857	Debian Security Update for nss (DSA 3688-1)	Vulnerability - level 3	Vuln
175876	Debian Security Update for curl (DSA 3705-1)	Vulnerability - level 3	Vuln
175900	Debian Security Update for openssl (DSA 2908-1)	Vulnerability - level 3	Vuln
175901	Debian Security Update for openssl (DSA 2998-1)	Vulnerability - level 3	Vuln
175902	Debian Security Update for Linux (DSA 2745-1)	Vulnerability - level 3	Vuln
175908	Debian Security Update for openssl (DLA-33-1)	Vulnerability - level 3	Vuln
175909	Debian Security Update for openssl (DLA-421-1)	Vulnerability - level 4	Vuln
175938	Debian Security Update for tiff (DSA 3762-1)	Vulnerability - level 3	Vuln
175985	Debian Security Update for pidgin (DSA 3806-1)	Vulnerability - level 3	Vuln
176098	Debian Security Update for openjdk-8 (DSA 3919-1)	Vulnerability - level 3	Vuln
176133	Debian Security Update for openjdk-7 (DSA 3954-1)	Vulnerability - level 3	Vuln
176140	Debian Security Update for mercurial (DSA 3963-1)	Vulnerability - level 3	Vuln
176179	Debian Security Update for wpa (DSA 3999-1) (KRACK Attack)	Vulnerability - level 4	Vuln
176196	Debian Security Update for openssl1.0 (DSA 4017-1)	Vulnerability - level 3	Vuln
176197	Debian Security Update for openssl (DSA 4018-1)	Vulnerability - level 3	Vuln
176251	Debian Security Update for Open Secure Sockets Layer (OpenSSL1.0) (DSA 4065-1)	Vulnerability - level 3	Vuln
176296	Debian Security Update for quagga (DSA 4115-1)	Vulnerability - level 3	Vuln
176443	Debian Security Update for Linux (DSA 4266-1)	Vulnerability - level 5	Vuln
176455	Debian Security Update for intel-microcode (DSA 4273-1)	Vulnerability - level 3	Vuln
176469	Debian Security Update for curl (DSA 4286-1)	Vulnerability - level 3	Vuln
176476	Debian Security Update for intel-microcode (DSA 4273-2)	Vulnerability - level 3	Vuln

176521	Debian Security Update for curl (DSA 4331-1)	Vulnerability - level 3	Vuln
176538	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 4348-1)	Vulnerability - level 3	Vuln
176545	Debian Security Update for Open Secure Sockets Layer (OpenSSL1.0) (DSA 4355-1)	Vulnerability - level 3	Vuln
176577	Debian Security Update for rssh (DSA 4382-1)	Vulnerability - level 3	Vuln
176578	Debian Security Update for libvncserver (DSA 4383-1)	Vulnerability - level 3	Vuln
176636	Debian Security Update for nss (DLA 1704-1)	Vulnerability - level 3	Vuln
176658	Debian Security Update for rssh (DLA 1660-1)	Vulnerability - level 4	Vuln
176726	Debian Security Update for libvncserver (DLA 1652-1)	Vulnerability - level 4	Vuln
176765	Debian Security Update for gpsd (DLA 1738-1)	Vulnerability - level 3	Vuln
176790	Debian Security Update for libvncserver (DLA 1617-1)	Vulnerability - level 4	Vuln
176814	Debian Security Update for curl (DLA 1568-1)	Vulnerability - level 4	Vuln
176821	Debian Security Update for firmware-nonfree (DLA 1573-1)	Vulnerability - level 5	Vuln
176872	Debian Security Update for drupal7 (DSA 4434-1)	Vulnerability - level 3	Vuln
176892	Debian Security Update for jquery (DLA 1777-1)	Vulnerability - level 3	Vuln
176919	Debian Security Update for mediawiki (DSA 4460-1)	Vulnerability - level 3	Vuln
176940	Debian Security Update for drupal7 (DLA 1797-1)	Vulnerability - level 4	Vuln
177021	Debian Security Update for python2.7 (DLA 1834-1)	Vulnerability - level 3	Vuln
177022	Debian Security Update for python3.4 (DLA 1835-1)	Vulnerability - level 3	Vuln
177068	Debian Security Update for subversion (DSA 4490-1)	Vulnerability - level 3	Vuln
177095	Debian Security Update for tomcat8 (DLA 1883-1)	Vulnerability - level 4	Vuln
177123	Debian Security Update for git-annex (DLA 1495-1)	Vulnerability - level 5	Vuln
177124	Debian Security Update for qemu (DLA 1497-1)	Vulnerability - level 4	Vuln
177125	Debian Security Update for curl (DLA 1498-1)	Vulnerability - level 5	Vuln
177126	Debian Security Update for openssh (DLA 1500-1)	Vulnerability - level 4	Vuln
177130	Debian Security Update for openssh (DLA 1500-2)	Vulnerability - level 4	Vuln
177133	Debian Security Update for intel-microcode (DLA 1506-1)	Vulnerability - level 3	Vuln
177145	Debian Long Term Support (LTS) Security Update for PolarSSL (DLA 1518-1)	Vulnerability - level 3	Vuln
177158	Debian Security Update for linux-4.9 (DLA 1466-1)	Vulnerability - level 3	Vuln
177193	Debian Security Update for linux-4.9 (DLA 1423-1)	Vulnerability - level 3	Vuln
177208	Debian Security Update for tomcat7 (DLA 1400-1)	Vulnerability - level 4	Vuln
177221	Debian Security Update for wpa (DLA 1462-1)	Vulnerability - level 2	Vuln
177252	Debian Security Update for intel-microcode (DLA 1446-1)	Vulnerability - level 3	Vuln
177256	Debian Long Term Support (LTS) Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 1449-1)	Vulnerability - level 3	Vuln
177301	Debian Security Update for subversion (DLA 1903-1)	Vulnerability - level 3	Vuln
177351	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 1932-1)	Vulnerability - level 3	Vuln
177363	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 4539-1)	Vulnerability - level 3	Vuln
177364	Debian Security Update for Open Secure Sockets Layer (OpenSSL1.0) (DSA 4540-1)	Vulnerability - level 3	Vuln
177479	Debian Security Update for libvncserver (DLA 1977-1)	Vulnerability - level 3	Vuln
177480	Debian Security Update for italc (DLA 1979-1)	Vulnerability - level 3	Vuln
177481	Debian Security Update for nss (DSA 4579-1)	Vulnerability - level 3	Vuln
177505	Debian Security Update for nss (DLA 2008-1)	Vulnerability - level 3	Vuln
177555	Debian Security Update for tightvnc (DLA 2045-1)	Vulnerability - level 4	Vuln
177566	Debian Security Update for libxml2 (DLA 2048-1)	Vulnerability - level 3	Vuln
177580	Debian Security Update for tomcat8 (DSA 4596-1)	Vulnerability - level 3	Vuln
177653	Debian Security Update for proftpd-dfsg (DSA 4635-1)	Vulnerability - level 3	Vuln
177669	Debian Security Update for proftpd-dfsg (DLA 2115-1)	Vulnerability - level 3	Vuln
177670	Debian Security Update for otrs2 (DLA 2118-1)	Vulnerability - level 3	Vuln
177679	Debian Security Update for proftpd-dfsg (DLA 2115-2)	Vulnerability - level 4	Vuln
177693	Debian Security Update for chromium (DSA 4638-1)	Vulnerability - level 3	Vuln
177698	Debian Security Update for libvncserver (DLA 2146-1)	Vulnerability - level 3	Vuln
177803	Debian Security Update for libreswan (DSA 4684-1)	Vulnerability - level 3	Vuln
177842	Debian Security Update for nodejs (DSA 4696-1)	Vulnerability - level 3	Vuln

177843	Debian Security Update for linux(DSA 4698-1)	Vulnerability - level 3	Vuln
177844	Debian Security Update for Linux Kernel (DSA 4699-1)	Vulnerability - level 3	Vuln
177845	Debian Security Update for intel-microcode (DSA 4701-1)	Vulnerability - level 3	Vuln
177859	Debian Security Update for linux (DLA 2241-1)	Vulnerability - level 3	Vuln
177860	Debian Security Update for linux-4.9 (DLA 2242-1)	Vulnerability - level 3	Vuln
177861	Debian Security Update for linux (DLA 2241-2)	Vulnerability - level 3	Vuln
177870	Debian Security Update for intel-microcode (DLA 2248-1)	Vulnerability - level 2	Vuln
177879	Debian Security Update for vino (DLA 2014-1)	Vulnerability - level 4	Vuln
177893	Debian Security Update for tightvnc (DLA 2045-1)	Vulnerability - level 4	Vuln
177920	Debian Security Update for mcabber (DLA 2260-1)	Vulnerability - level 3	Vuln
177924	Debian Security Update for libvncserver (DLA 2264-1)	Vulnerability - level 4	Vuln
177949	Debian Security Update for python3.5 (DLA 2280-1)	Vulnerability - level 3	Vuln
177969	Debian Security Update for grub2 (DSA 4735-2)	Vulnerability - level 4	Vuln
178035	Debian Security Update for python2.7 (DLA 2337-1)	Vulnerability - level 3	Vuln
178038	Debian Security Update for sqlite3 (DLA 2340-1)	Vulnerability - level 3	Vuln
178045	Debian Security Update for libvncserver (DLA 2347-1)	Vulnerability - level 3	Vuln
178076	Debian Security Update for libxml2 (DLA 2369-1)	Vulnerability - level 3	Vuln
178134	Debian Security Update for nss (DLA 2388-1)	Vulnerability - level 5	Vuln
178215	Debian Security Update for openldap (DSA 4792-1)	Vulnerability - level 4	Vuln
178251	Debian Security Update for openldap (DLA 2481-1)	Vulnerability - level 3	Vuln
178254	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 4807-1)	Vulnerability - level 3	Vuln
178263	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 2492-1)	Vulnerability - level 3	Vuln
178264	Debian Security Update for Open Secure Sockets Layer (OpenSSL1.0) (DLA 2493-1)	Vulnerability - level 3	Vuln
178288	Debian Security Update for linux (DLA 2494-1)	Vulnerability - level 3	Vuln
178289	Debian Security Update for curl (DLA 2500-1)	Vulnerability - level 3	Vuln
178303	Debian Security Update for linux (DLA 2483-1)	Vulnerability - level 3	Vuln
178372	Debian Security Update for Open Secure Sockets Layer (OpenSSL1.0) (DLA 2378-1)	Vulnerability - level 2	Vuln
178376	Debian Security Update for openvswitch (DSA 4836-1)	Vulnerability - level 3	Vuln
178387	Debian Security Update for ansible (DLA 2535-1)	Vulnerability - level 4	Vuln
178399	Debian Security Update for openldap (DSA 4845-1)	Vulnerability - level 3	Vuln
178407	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 2563-1)	Vulnerability - level 3	Vuln
178411	Debian Security Update for Open Secure Sockets Layer (OpenSSL1.0) (DLA 2565-1)	Vulnerability - level 3	Vuln
178416	Debian Security Update for bind9 (DLA 2568-1)	Vulnerability - level 3	Vuln
178419	Debian Security Update for openvswitch (DLA 2571-1)	Vulnerability - level 4	Vuln
178423	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 4855-1)	Vulnerability - level 3	Vuln
178426	Debian Security Update for bind9 (DSA 4857-1)	Vulnerability - level 3	Vuln
178435	Debian Security Update for grub2 (DSA-4867-1)	Vulnerability - level 5	Vuln
178444	Debian Security Update for dnsmasq (DSA 4844-1)	Vulnerability - level 4	Vuln
178453	Debian Security Update for nodejs (DSA 4863-1)	Vulnerability - level 3	Vuln
178461	Debian Security Update for openldap (DLA 2544-1)	Vulnerability - level 3	Vuln
178462	Debian Security Update for intel-microcode (DLA 2546-1)	Vulnerability - level 2	Vuln
178486	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 4875-1)	Vulnerability - level 4	Vuln
178499	Debian Security Update for dnsmasq (DLA 2604-1)	Vulnerability - level 3	Vuln
178522	Debian Security Update for curl (DSA 4881-1)	Vulnerability - level 3	Vuln
178573	Debian Security Update for bind9 (DSA 4909-1)	Vulnerability - level 3	Vuln
178586	Debian Security Update for libxml2 (DLA 2653-1)	Vulnerability - level 3	Vuln
178594	Debian Security Update for bind9 (DLA 2647-1)	Vulnerability - level 3	Vuln
178598	Debian Security Update for postgresql-9.6 (DLA 2662-1)	Vulnerability - level 3	Vuln
178608	Debian Security Update for libxml2 (DLA 2669-1)	Vulnerability - level 3	Vuln
178614	Debian Security Update for grub2 (DSA 4867-1)	Vulnerability - level 4	Vuln
178617	Debian Security Update for postgresql-11 (DSA 4915-1)	Vulnerability - level 3	Vuln

178679	Debian Security Update for linux-4.19 (DLA 2690-1)	Vulnerability - level 4	Vuln
178680	Debian Security Update for linux (DLA 2689-1)	Vulnerability - level 4	Vuln
178683	Debian Security Update for intel-microcode (DSA 4934-1)	Vulnerability - level 3	Vuln
178699	Debian Security Update for apache2 (DSA 4937-1)	Vulnerability - level 4	Vuln
178701	Debian Security Update for apache2 (DLA 2706-1)	Vulnerability - level 4	Vuln
178725	Debian Security Update for intel-microcode (DLA 2718-1)	Vulnerability - level 2	Vuln
178774	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 4963-1)	Vulnerability - level 3	Vuln
178810	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 2766-1)	Vulnerability - level 3	Vuln
178815	Debian Security Update for apache2 (DLA 2776-1)	Vulnerability - level 4	Vuln
178819	Debian Security Update for apache2 (DSA 4982-1)	Vulnerability - level 4	Vuln
178839	Debian Security Update for nghttp2 (DLA 2786-1)	Vulnerability - level 3	Vuln
178849	Debian Security Update for postgresql-9.6 (DLA 2751-1)	Vulnerability - level 2	Vuln
178853	Debian Security Update for Open Secure Sockets Layer1.0 (OpenSSL1.0) (DLA 2774-1)	Vulnerability - level 3	Vuln
178855	Debian Security Update for bind9 (DSA 4994-1)	Vulnerability - level 3	Vuln
178863	Debian Security Update for bind9 (DLA 2807-1)	Vulnerability - level 3	Vuln
178875	Debian Security Update for gpsd (DLA 2795-1)	Vulnerability - level 3	Vuln
178878	Debian Security Update for containerd (DSA 5002-1)	Vulnerability - level 4	Vuln
178894	Debian Security Update for node-tar (DSA 5008-1)	Vulnerability - level 2	Vuln
178909	Debian Security Update for mbedtls (DLA 2826-1)	Vulnerability - level 3	Vuln
178943	Debian Security Update for linux (DLA 2843-1)	Vulnerability - level 4	Vuln
179017	Debian Security Update for golang-1.8 (DLA 2891-1)	Vulnerability - level 4	Vuln
179018	Debian Security Update for golang-1.7 (DLA 2892-1)	Vulnerability - level 4	Vuln
179044	Debian Security Update for expat (DLA 2904-1)	Vulnerability - level 5	Vuln
179068	Debian Security Update for expat (DSA 5073-1)	Vulnerability - level 5	Vuln
179091	Debian Security Update for expat (DSA 5085-1)	Vulnerability - level 3	Vuln
179107	Debian Security Update for expat (DLA 2935-1)	Vulnerability - level 5	Vuln
179115	Debian Security Update for linux (DSA 5095-1)	Vulnerability - level 4	Vuln
179117	Debian Security Update for linux (DSA 5096-1)	Vulnerability - level 4	Vuln
179118	Debian Security Update for linux (DLA 2940-1)	Vulnerability - level 4	Vuln
179119	Debian Security Update for linux-4.19 (DLA 2941-1)	Vulnerability - level 4	Vuln
179133	Debian Security Update for bind9 (DLA 2955-1)	Vulnerability - level 4	Vuln
179135	Debian Security Update for bind9 (DLA 2955-2)	Vulnerability - level 4	Vuln
179142	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 5103-1)	Vulnerability - level 3	Vuln
179144	Debian Security Update for bind9 (DSA 5105-1)	Vulnerability - level 4	Vuln
179151	Debian Security Update for apache2 (DLA 2960-1)	Vulnerability - level 5	Vuln
179155	Debian Security Update for bind9 (CVE-2022-0396)	Vulnerability - level 3	Vuln
179176	Debian Security Update for libxml2 (DLA 2972-1)	Vulnerability - level 4	Vuln
179202	Debian Security Update for apache2 (CVE-2022-22720)	Vulnerability - level 5	Vuln
179203	Debian Security Update for apache2 (CVE-2022-23943)	Vulnerability - level 5	Vuln
179208	Debian Security Update for libxml2 (CVE-2022-23308)	Vulnerability - level 4	Vuln
179209	Debian Security Update for golang-1.15 (CVE-2022-24921)	Vulnerability - level 4	Vuln
179217	Debian Security Update for linux (CVE-2022-23038)	Vulnerability - level 4	Vuln
179219	Debian Security Update for linux (CVE-2022-23036)	Vulnerability - level 4	Vuln
179223	Debian Security Update for linux (CVE-2022-23037)	Vulnerability - level 4	Vuln
179231	Debian Security Update for linux (CVE-2022-23042)	Vulnerability - level 4	Vuln
179232	Debian Security Update for linux (CVE-2022-23040)	Vulnerability - level 4	Vuln
179234	Debian Security Update for linux (CVE-2022-23039)	Vulnerability - level 4	Vuln
179235	Debian Security Update for linux (CVE-2022-23041)	Vulnerability - level 4	Vuln
179242	Debian Security Update for linux (CVE-2022-1199)	Vulnerability - level 3	Vuln
179251	Debian Security Update for golang-1.7 (DLA 2985-1)	Vulnerability - level 5	Vuln
179252	Debian Security Update for golang-1.8 (DLA 2986-1)	Vulnerability - level 5	Vuln
179258	Debian Security Update for linux (DSA 5127-1)	Vulnerability - level 4	Vuln
179259	Debian Security Update for Open Virtual Private Network (OpenVPN) (DLA 2992-1)	Vulnerability - level 5	Vuln

179286	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 3008-1)	Vulnerability - level 5	Vuln
179294	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 5139-1)	Vulnerability - level 5	Vuln
179371	Debian Security Update for linux (DSA 5161-1)	Vulnerability - level 4	Vuln
179493	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 5169-1)	Vulnerability - level 4	Vuln
179499	Debian Security Update for docker.io (CVE-2021-41092)	Vulnerability - level 4	Vuln
179511	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2021-3449)	Vulnerability - level 3	Vuln
179528	Debian Security Update for node-tar (CVE-2021-32804)	Vulnerability - level 4	Vuln
179583	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2021-23841)	Vulnerability - level 3	Vuln
179594	Debian Security Update for golang-1.15 (CVE-2021-44717)	Vulnerability - level 2	Vuln
179618	Debian Security Update for golang-1.15 (CVE-2021-39293)	Vulnerability - level 4	Vuln
179668	Debian Security Update for docker.io (CVE-2021-41089)	Vulnerability - level 3	Vuln
179690	Debian Security Update for nodejs (CVE-2021-22930)	Vulnerability - level 5	Vuln
179693	Debian Security Update for grub2 (CVE-2021-20225)	Vulnerability - level 3	Vuln
179754	Debian Security Update for nodejs (CVE-2021-22883)	Vulnerability - level 4	Vuln
179764	Debian Security Update for bind9 (CVE-2021-25216)	Vulnerability - level 5	Vuln
179907	Debian Security Update for linux (CVE-2021-26401)	Vulnerability - level 3	Vuln
179935	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2021-3450)	Vulnerability - level 4	Vuln
179946	Debian Security Update for linux (CVE-2021-20317)	Vulnerability - level 2	Vuln
179969	Debian Security Update for libxml2 (CVE-2021-3517)	Vulnerability - level 4	Vuln
179980	Debian Security Update for apache2 (CVE-2021-26691)	Vulnerability - level 5	Vuln
180038	Debian Security Update for golang-1.15 (CVE-2021-44716)	Vulnerability - level 4	Vuln
180040	Debian Security Update for picolibc (CVE-2021-3420)	Vulnerability - level 5	Vuln
180134	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2021-23839)	Vulnerability - level 2	Vuln
180141	Debian Security Update for postgresql-13 (CVE-2021-32028)	Vulnerability - level 3	Vuln
180182	Debian Security Update for libxml2 (CVE-2021-3518)	Vulnerability - level 4	Vuln
180242	Debian Security Update for libxml2 (CVE-2021-3537)	Vulnerability - level 3	Vuln
180282	Debian Security Update for linux (DLA 3065-1)	Vulnerability - level 5	Vuln
180333	Debian Security Update for golang-1.15 (CVE-2021-36221)	Vulnerability - level 3	Vuln
180392	Debian Security Update for bind9 (CVE-2021-25215)	Vulnerability - level 4	Vuln
180469	Debian Security Update for golang-1.15 (CVE-2021-41771)	Vulnerability - level 4	Vuln
180473	Debian Security Update for postgresql-13 (CVE-2021-32027)	Vulnerability - level 4	Vuln
180493	Debian Security Update for bind9 (CVE-2021-25214)	Vulnerability - level 3	Vuln
180540	Debian Security Update for libxml2 (CVE-2021-3541)	Vulnerability - level 3	Vuln
180566	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2021-23840)	Vulnerability - level 4	Vuln
180570	Debian Security Update for grub2 (CVE-2021-20233)	Vulnerability - level 4	Vuln
180594	Debian Security Update for node-tar (CVE-2021-32803)	Vulnerability - level 4	Vuln
180605	Debian Security Update for linux (DSA 5173-1)	Vulnerability - level 4	Vuln
180783	Debian Security Update for dlt-daemon (CVE-2020-36244)	Vulnerability - level 5	Vuln
180834	Debian Security Update for apache2 (CVE-2022-26377)	Vulnerability - level 4	Vuln
180835	Debian Security Update for apache2 (CVE-2022-31813)	Vulnerability - level 5	Vuln
180850	Debian Security Update for linux (CVE-2022-32296)	Vulnerability - level 2	Vuln
180884	Debian Security Update for linux (CVE-2022-2380)	Vulnerability - level 3	Vuln
180938	Debian Security Update for linux (DSA 5207-1)	Vulnerability - level 4	Vuln
181002	Debian Security Update for linux-5.10 (DLA 3102-1)	Vulnerability - level 4	Vuln
181091	Debian Security Update for linux (DLA 3131-1)	Vulnerability - level 4	Vuln
181111	Debian Security Update for nodejs (DLA 3137-1)	Vulnerability - level 5	Vuln
181247	Debian Security Update for inetutils (DLA 3205-1)	Vulnerability - level 4	Vuln
181308	Debian Security Update for dlt-daemon (DLA 3231-1)	Vulnerability - level 5	Vuln
181317	Debian Security Update for node-tar (DLA 3237-1)	Vulnerability - level 4	Vuln
181446	Debian Security Update for mbedtls (DLA 3249-1)	Vulnerability - level 5	Vuln
181502	Debian Security Update for nodejs (DSA 5326-1)	Vulnerability - level 5	Vuln

181546	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DSA 5343-1)	Vulnerability - level 3	Vuln
181593	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (DLA 3325-1)	Vulnerability - level 5	Vuln
181728	Debian Security Update for lldpd (DLA 3388-1)	Vulnerability - level 4	Vuln
181730	Debian Security Update for lldpd (DLA 3389-1)	Vulnerability - level 4	Vuln
181743	Debian Security Update for golang-1.11 (DLA 3395-1)	Vulnerability - level 5	Vuln
181942	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2021-4160)	Vulnerability - level 3	Vuln
181967	Debian Security Update for busybox (CVE-2021-42382)	Vulnerability - level 4	Vuln
181983	Debian Security Update for busybox (CVE-2021-42386)	Vulnerability - level 4	Vuln
181994	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-2068)	Vulnerability - level 5	Vuln
182043	Debian Security Update for linux (CVE-2022-36879)	Vulnerability - level 3	Vuln
182064	Debian Security Update for apache2 (CVE-2021-34798)	Vulnerability - level 4	Vuln
182136	Debian Security Update for busybox (CVE-2021-42379)	Vulnerability - level 4	Vuln
182164	Debian Security Update for expat (CVE-2022-22824)	Vulnerability - level 5	Vuln
182233	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2023-0286)	Vulnerability - level 4	Vuln
182249	Debian Security Update for dcmtk (CVE-2022-2120)	Vulnerability - level 5	Vuln
182327	Debian Security Update for expat (CVE-2022-25314)	Vulnerability - level 4	Vuln
182338	Debian Security Update for linux (CVE-2022-1516)	Vulnerability - level 3	Vuln
182376	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2021-3712)	Vulnerability - level 4	Vuln
182419	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2023-0215)	Vulnerability - level 4	Vuln
182460	Debian Security Update for nodejs (CVE-2021-22940)	Vulnerability - level 4	Vuln
182562	Debian Security Update for node-tar (CVE-2021-37701)	Vulnerability - level 4	Vuln
182673	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-4450)	Vulnerability - level 4	Vuln
182740	Debian Security Update for node-tar (CVE-2021-37712)	Vulnerability - level 4	Vuln
182780	Debian Security Update for expat (CVE-2022-23852)	Vulnerability - level 5	Vuln
182916	Debian Security Update for linux (CVE-2022-1974)	Vulnerability - level 2	Vuln
183018	Debian Security Update for busybox (CVE-2021-42375)	Vulnerability - level 3	Vuln
183023	Debian Security Update for busybox (CVE-2021-42383)	Vulnerability - level 4	Vuln
183084	Debian Security Update for bind9 (CVE-2021-25220)	Vulnerability - level 3	Vuln
183097	Debian Security Update for dcmtk (CVE-2022-2119)	Vulnerability - level 5	Vuln
183107	Debian Security Update for linux (CVE-2022-26490)	Vulnerability - level 4	Vuln
183110	Debian Security Update for linux (CVE-2022-1729)	Vulnerability - level 4	Vuln
183156	Debian Security Update for expat (CVE-2022-23990)	Vulnerability - level 4	Vuln
183162	Debian Security Update for e2fsprogs (CVE-2022-1304)	Vulnerability - level 4	Vuln
183164	Debian Security Update for fastdds (CVE-2021-38425)	Vulnerability - level 5	Vuln
183168	Debian Security Update for apache2 (CVE-2021-39275)	Vulnerability - level 5	Vuln
183232	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-1292)	Vulnerability - level 5	Vuln
183248	Debian Security Update for cyclonedds (CVE-2021-38443)	Vulnerability - level 5	Vuln
183351	Debian Security Update for samba (CVE-2023-0614)	Vulnerability - level 3	Vuln
183364	Debian Security Update for cyclonedds (CVE-2021-38441)	Vulnerability - level 5	Vuln
183402	Debian Security Update for npm (CVE-2021-39135)	Vulnerability - level 4	Vuln
183465	Debian Security Update for expat (CVE-2022-22823)	Vulnerability - level 5	Vuln
183596	Debian Security Update for expat (CVE-2022-22822)	Vulnerability - level 5	Vuln
183606	Debian Security Update for containerd (CVE-2021-41103)	Vulnerability - level 4	Vuln
183654	Debian Security Update for busybox (CVE-2021-42385)	Vulnerability - level 4	Vuln
183667	Debian Security Update for npm (CVE-2021-39134)	Vulnerability - level 4	Vuln
183669	Debian Security Update for busybox (CVE-2021-42377)	Vulnerability - level 5	Vuln
183681	Debian Security Update for linux (CVE-2022-1353)	Vulnerability - level 4	Vuln
183695	Debian Security Update for bind9 (CVE-2021-25219)	Vulnerability - level 3	Vuln
183796	Debian Security Update for expat (CVE-2022-22827)	Vulnerability - level 4	Vuln

183852	Debian Security Update for Open Virtual Private Network (OpenVPN) (CVE-2022-0547)	Vulnerability - level 5	Vuln
183869	Debian Security Update for samba (CVE-2023-0225)	Vulnerability - level 2	Vuln
183872	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2021-3711)	Vulnerability - level 5	Vuln
183949	Debian Security Update for linux (CVE-2022-0001)	Vulnerability - level 3	Vuln
183975	Debian Security Update for linux (CVE-2022-0002)	Vulnerability - level 3	Vuln
184021	Debian Security Update for busybox (CVE-2021-42373)	Vulnerability - level 3	Vuln
184089	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-2097)	Vulnerability - level 3	Vuln
184162	Debian Security Update for busybox (CVE-2021-42378)	Vulnerability - level 4	Vuln
184296	Debian Security Update for nodejs (CVE-2022-32212)	Vulnerability - level 4	Vuln
184546	Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-4304)	Vulnerability - level 3	Vuln
184547	Debian Security Update for expat (CVE-2022-22826)	Vulnerability - level 4	Vuln
184570	Debian Security Update for busybox (CVE-2021-42376)	Vulnerability - level 3	Vuln
184639	Debian Security Update for busybox (CVE-2021-42381)	Vulnerability - level 4	Vuln
184643	Debian Security Update for expat (CVE-2022-25313)	Vulnerability - level 3	Vuln
184672	Debian Security Update for expat (CVE-2022-25235)	Vulnerability - level 5	Vuln
184687	Debian Security Update for busybox (CVE-2021-42384)	Vulnerability - level 4	Vuln
184734	Debian Security Update for samba (CVE-2023-0922)	Vulnerability - level 3	Vuln
184740	Debian Security Update for linux (CVE-2022-1975)	Vulnerability - level 3	Vuln
184766	Debian Security Update for linux (CVE-2022-28390)	Vulnerability - level 4	Vuln
184795	Debian Security Update for busybox (CVE-2021-42380)	Vulnerability - level 4	Vuln
184824	Debian Security Update for dcmthk (CVE-2022-2121)	Vulnerability - level 3	Vuln
185011	HP-UX Running Java Remote Code Execution Vulnerability (HPSBUX02824)	Vulnerability - level 3	Vuln
185016	HP-UX Running OpenSSL Remote Denial of Service and Unauthorized Disclosure Vulnerability (HPSBUX02856)	Vulnerability - level 3	Vuln
185017	HP-UX Running Java Multiple Vulnerabilities (HPSBUX02857)	Vulnerability - level 3	Vuln
185018	HP-UX Apache Running Tomcat Servlet Engine Multiple Vulnerabilities (HPSBUX02860)	Vulnerability - level 3	Vuln
185021	HP-UX Running Apache Multiple Vulnerabilities (HPSBUX02866)	Vulnerability - level 3	Vuln
185022	HP-UX Running Java Multiple Vulnerabilities (HPSBUX02867)	Vulnerability - level 4	Vuln
185023	HP-UX Running CIFS Server Remote Denial of Service Vulnerability (HPSBUX02204)	Vulnerability - level 3	Vuln
185024	HP-UX Running BIND Remote Denial of Service Vulnerability (HPSBUX02876)	Vulnerability - level 3	Vuln
185026	HP-UX Apache Web Server Multiple Vulnerabilities (HPSBUX02645)	Vulnerability - level 3	Vuln
185027	HP-UX Running Apache Remote Code Execution Vulnerability (HPSBUX02292)	Vulnerability - level 4	Vuln
185029	HP-UX Running OpenSSL Multiple Vulnerabilities (HPSBUX02517)	Vulnerability - level 3	Vuln
185030	HP-UX Running OpenSSL Multiple Vulnerabilities (HPSBUX02174)	Vulnerability - level 3	Vuln
185031	HP-UX Running Kerberos Multiple Vulnerabilities (HPSBUX02421)	Vulnerability - level 3	Vuln
185033	HP-UX Running HP CIFS Server (Samba) Remote Execution of Arbitrary Code (HPSBUX02341)	Vulnerability - level 3	Vuln
185035	HP-UX Running HP CIFS Server (Samba) Remote Execution of Arbitrary Code Vulnerability (HPSBUX02316)	Vulnerability - level 3	Vuln
185038	HP-UX Secure Shell Remote Unauthorized Denial of Service Vulnerability (HPSBUX02178)	Vulnerability - level 3	Vuln
185039	HP-UX Running BIND Remote Denial of Service Vulnerability (HPSBUX02219)	Vulnerability - level 3	Vuln
185040	HP-UX Running OpenSSL Multiple Vulnerabilities (HPSBUX02174)	Vulnerability - level 3	Vuln
185046	HP-UX Running Java Multiple Vulnerabilities (HPSBUX02889)	Vulnerability - level 4	Vuln
185049	HP-UX Apache Web Server Remote Denial of Service Vulnerability (HPSBUX02909)	Vulnerability - level 3	Vuln
185051	HP-UX Running Java5 Multiple Vulnerabilities (HPSBUX02922)	Vulnerability - level 4	Vuln

185054	HP-UX Apache Web Server Multiple Vulnerabilities (HPSBUX02927)	Vulnerability - level 3	Vuln
185071	HP-UX Running Tomcat Servlet Engine Multiple Vulnerabilities (HPSBUX02466)	Vulnerability - level 3	Vuln
185074	HP-UX Running Java Multiple Vulnerabilities (HPSBUX02476)	Vulnerability - level 3	Vuln
185076	HP-UX Running Apache Web Server Suite Multiple Vulnerabilities (HPSBUX02431)	Vulnerability - level 3	Vuln
185079	HP-UX Running PAM Kerberos Multiple Vulnerabilities (HPSBUX02415)	Vulnerability - level 3	Vuln
185080	HP-UX Running Java Multiple Vulnerabilities (HPSBUX02411)	Vulnerability - level 4	Vuln
185081	HP-UX Running OpenSSL Multiple Vulnerabilities (HPSBUX03046)	Vulnerability - level 4	Vuln
185083	HP-UX Running OpenSSL Multiple Vulnerabilities (HPSBUX03095)	Vulnerability - level 3	Vuln
185085	HP-UX running Java 7 Multiple Vulnerabilities (HPSBUX03091)	Vulnerability - level 4	Vuln
185086	HP-UX running Java6, Multiple Vulnerabilities(HPSBUX03092)	Vulnerability - level 4	Vuln
185089	HP-UX Apache Server Suite Multiple Vulnerabilities (HPSBUX03102)	Vulnerability - level 3	Vuln
185097	HP-UX Running NTP Multiple Vulnerabilities (HPSBUX03240)	Vulnerability - level 3	Vuln
185099	HP-UX Running OpenSSL Multiple Vulnerabilities (HPSBUX03244)	Vulnerability - level 4	Vuln
185103	HP-UX Running NTP Remote Denial of Service Vulnerability	Vulnerability - level 3	Vuln
185104	HP-UX Running OpenSSL Remote Denial of Service Vulnerability (HPSBUX03334)	Vulnerability - level 4	Vuln
185105	HP-UX Apache Tomcat Remote Denial of Service Vulnerability (HPSBUX03341)	Vulnerability - level 3	Vuln
185106	HP-UX Apache Web Server Suite Remote Denial of Service Vulnerability (HPSBUX03337)	Vulnerability - level 3	Vuln
185110	HP-UX Web Server Suite running Apache Multiple Vulnerabilities (HPSBUX03512)	Vulnerability - level 3	Vuln
185111	HP-UX running OpenSSL Remote Disclosure of Information Vulnerability (HPSBUX03388)	Vulnerability - level 4	Vuln
185118	HP-UX Apache Web Server Suite Remote Denial of Service Vulnerability (HPSBUX03435)	Vulnerability - level 3	Vuln
185121	HP-UX Apache Tomcat Multiple Vulnerabilities (HPSBUX03561)	Vulnerability - level 4	Vuln
185124	HPE HP-UX CIFS-Server Multiple Vulnerabilities (HPSBUX03574)	Vulnerability - level 3	Vuln
185126	HPE HP-UX running Apache Tomcat 7 Multiple Remote Vulnerabilities (HPSBUX03606)	Vulnerability - level 3	Vuln
185129	HP-UX Tomcat-based Servlet Engine Remote Denial of Service Vulnerability (HPSBUX03665)	Vulnerability - level 4	Vuln
185132	HP-UX NTP service running ntpd Multiple Vulnerabilities (HPESBUX03706)	Vulnerability - level 4	Vuln
185139	HP-UX Secure Shell Multiple Remote Vulnerabilities (HPESBUX03818)	Vulnerability - level 3	Vuln
19143	InnerMedia DynaZip ZIP Archive Handling Multiple Buffer Overflow Vulnerabilities	Vulnerability - level 3	
19143	MySQL User-Defined Function Buffer Overflow Vulnerability	Vulnerability - level 3	Vuln
19236	Microsoft SQL Server Could Allow Elevation of Privilege (MS08-040)	Vulnerability - level 3	Practice
19236	X-Scripts X-Poll Top.PHP SQL Injection Vulnerability	Vulnerability - level 3	
19238	Ajax Chat Multiple Remote Vulnerabilities	Vulnerability - level 4	
19238	Oracle July 2008 Security Update Multiple Vulnerabilities	Vulnerability - level 4	Practice
19463	IBM WebSphere Application Server 6.1.0 Multiple Vulnerabilities	Vulnerability - level 4	
19463	Oracle April 2009 Security Update Multiple Vulnerabilities	Vulnerability - level 4	Practice
19484	Nokia Browser HTML Denial of Service Vulnerability	Vulnerability - level 4	
19484	Oracle July 2009 Security Update Multiple Vulnerabilities	Vulnerability - level 4	Practice
195006	Ubuntu Security Notification for Linux, Linux-source-2.6.15 Vulnerabilities (USN-864-1)	Vulnerability - level 4	Vuln
195007	Ubuntu Security Notification for Bind9 Vulnerability (USN-865-1)	Vulnerability - level 4	Vuln
195022	Ubuntu Security Notification for Krb5 Vulnerability (USN-879-1)	Vulnerability - level 3	Vuln
195023	Ubuntu Security Notification for Gimp Vulnerabilities (USN-880-1)	Vulnerability - level 3	Vuln

195039	Ubuntu Security Notification for Samba Vulnerability (USN-893-1)	Vulnerability - level 3	Vuln
195040	Ubuntu Security Notification for Fuse Vulnerability (USN-892-1)	Vulnerability - level 3	Vuln
195041	Ubuntu Security Notification for MySql-dfsg-5.0, MySQL-dfsg-5.1 Vulnerabilities (USN-897-1)	Vulnerability - level 4	Vuln
195043	Ubuntu Security Notification for Tomcat 6 Vulnerabilities (USN-899-1)	Vulnerability - level 3	Vuln
195044	Ubuntu Security Notification for Firefox 3.0, Xulrunner 1.9 Vulnerabilities (USN-895-1)	Vulnerability - level 3	Vuln
195045	Ubuntu Security Notification for Firefox 3.5, Xulrunner 1.9.1 Vulnerabilities (USN-896-1)	Vulnerability - level 3	Vuln
195046	Ubuntu Security Notification for Mysql-dfsg 5.0, Mysql-dfsg 5.1 Vulnerabilities (USN-897-1)	Vulnerability - level 3	Vuln
195048	Ubuntu Security Notification for Tomcat 6 Vulnerabilities (USN-899-1)	Vulnerability - level 3	Vuln
195054	Ubuntu Security Notification for Openoffice.org Vulnerabilities (USN-903-1)	Vulnerability - level 3	Vuln
195071	Ubuntu Security Notification for Krb5 Vulnerabilities (USN-916-1)	Vulnerability - level 3	Vuln
195077	Ubuntu Security Notification for Openjdk-6 Vulnerabilities (USN-923-1)	Vulnerability - level 4	Vuln
195090	Ubuntu Security Notification for Kdebase-Workspace Vulnerability (USN-932-1)	Vulnerability - level 3	Vuln
195095	Ubuntu Security Notification for Kdenetwork Vulnerability (USN-938-1)	Vulnerability - level 3	Vuln
195097	Ubuntu Security Notification for Krb5 Vulnerabilities (USN-940-1)	Vulnerability - level 3	Vuln
195103	Ubuntu Security Notification for Linux, Linux-source-2.6.15 Vulnerabilities (USN-947-1)	Vulnerability - level 3	Vuln
195109	Ubuntu Security Notification for TIFF Vulnerabilities (USN-954-1)	Vulnerability - level 3	Vuln
195111	Ubuntu Security Notification for Openjdk-6 Vulnerabilities (USN-814-1)	Vulnerability - level 3	Vuln
195133	Ubuntu Security Notification for Curl Vulnerability (USN-1346-1)	Vulnerability - level 3	Vuln
195162	Ubuntu Security Notification for T1lib Vulnerability (USN-1316-1)	Vulnerability - level 3	Vuln
195247	Ubuntu Security Notice for Linux-lts-Backport-Natty Vulnerabilities (USN-1256-1)	Vulnerability - level 2	Vuln
195277	Ubuntu Security Notification for Eglibc, Glibc Vulnerabilities (USN-1589-1)	Vulnerability - level 4	Vuln
195307	Ubuntu Security Notification for OpenSSL Vulnerabilities (USN-1732-1)	Vulnerability - level 4	Vuln
195328	Ubuntu Security Notification for Tomcat6, Tomcat7 Vulnerabilities (USN-1685-1)	Vulnerability - level 4	Vuln
195352	Ubuntu Security Notification for Perl Vulnerabilities (USN-1643-1)	Vulnerability - level 4	Vuln
195358	Ubuntu Security Notification for Tomcat6 Vulnerabilities (USN-1637-1)	Vulnerability - level 3	Vuln
195364	Ubuntu Security Notification for Libproxy Vulnerabilities (USN-1629-1)	Vulnerability - level 5	Vuln
195365	Ubuntu Security Notification for Bind9 Vulnerability (USN-1783-1)	Vulnerability - level 4	Vuln
195370	Ubuntu Security Notification for Postgresql-8.3, Postgresql-8.4, Postgresql-9.1 Vulnerabilities (USN-1789-1)	Vulnerability - level 3	Vuln
195373	Ubuntu Security Notification for Libxml2 Vulnerability (USN-1782-1)	Vulnerability - level 2	Vuln
195375	Ubuntu Security Notification for Apache2 Vulnerabilities (USN-1765-1)	Vulnerability - level 4	Vuln
195376	Ubuntu Security Notification for Php5 Vulnerability (USN-1761-1)	Vulnerability - level 3	Vuln
195381	Ubuntu Security Notification for Libxslt Vulnerabilities (USN-1595-1)	Vulnerability - level 4	Vuln
195383	Ubuntu Security Notification for Eglibc, Glibc Vulnerabilities (USN-1589-1)	Vulnerability - level 3	Vuln
195396	Ubuntu Security Notification for Openjdk-6 Vulnerabilities (USN-1819-1)	Vulnerability - level 4	Vuln

195400	Ubuntu Security Notification for Linux-ec2 Vulnerabilities (USN-1808-1)	Vulnerability - level 4	Vuln
195401	Ubuntu Security Notification for Linux Vulnerabilities (USN-1805-1)	Vulnerability - level 4	Vuln
195415	Ubuntu Security Notification for Linux-lts-raring Vulnerabilities (USN-1936-1)	Vulnerability - level 5	Vuln
195416	Ubuntu Security Notification for Linux Vulnerabilities (USN-1935-1)	Vulnerability - level 5	Vuln
195423	Ubuntu Security Notification for Linux Kernel Vulnerabilities (USN-1941-1)	Vulnerability - level 4	Vuln
195424	Ubuntu Security Notification for Linux Kernel (OMAP4) Vulnerabilities (USN-2076-1)	Vulnerability - level 4	Vuln
195433	Ubuntu Security Notification for Gnutls26 Vulnerability (USN-2127-1)	Vulnerability - level 4	Vuln
195443	Ubuntu Security Notification for Openssl Vulnerabilities (USN-2165-1) (Heartbleed Bug)	Vulnerability - level 4	Vuln
195445	Ubuntu Security Notification for Curl Vulnerabilities (USN-2167-1)	Vulnerability - level 4	Vuln
195450	Ubuntu Security Notification for MySQL Vulnerability (USN-2170-1)	Vulnerability - level 3	Vuln
195453	Ubuntu Security Notification for Linux Kernel (Quantal HWE) Vulnerabilities (USN-2175-1)	Vulnerability - level 4	Vuln
195454	Ubuntu Security Notification for Linux kernel (Raring HWE) Vulnerabilities (USN-2176-1)	Vulnerability - level 4	Vuln
195455	Ubuntu Security Notification for Linux kernel (Saucy HWE) Vulnerabilities (USN-2177-1)	Vulnerability - level 4	Vuln
195456	Ubuntu Security Notification for Linux Kernel Vulnerabilities (USN-2178-1)	Vulnerability - level 4	Vuln
195457	Ubuntu Security Notification for Linux Kernel Vulnerabilities (USN-2179-1)	Vulnerability - level 4	Vuln
195458	Ubuntu Security Notification for Linux Kernel (OMAP4) Vulnerabilities (USN-2180-1)	Vulnerability - level 4	Vuln
195459	Ubuntu Security Notification for Linux Kernel (OMAP4) Vulnerabilities (USN-2181-1)	Vulnerability - level 4	Vuln
195466	Ubuntu Security Notification for Unity Vulnerabilities (USN-2188-1)	Vulnerability - level 4	Vuln
195470	Ubuntu Security Notification for OpenSSL Vulnerabilities (USN-2192-1)	Vulnerability - level 3	Vuln
19548	Oracle April 2010 Security Update Multiple Vulnerabilities	Vulnerability - level 5	Practice
19548	Outreach Project Tool Remote File Include Vulnerability	Vulnerability - level 5	
195484	Ubuntu Security Notification for OpenStack Swift Vulnerability (USN-2207-1)	Vulnerability - level 3	Vuln
195488	Ubuntu Security Notification for OpenSSL Vulnerabilities (USN-2232-1)	Vulnerability - level 4	Vuln
195492	Ubuntu Security Notification for Python-django Vulnerabilities (USN-2212-1)	Vulnerability - level 4	Vuln
195505	Ubuntu Security Notification for Linux Vulnerabilities (USN-2221-1)	Vulnerability - level 4	Vuln
195510	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-2227-1)	Vulnerability - level 4	Vuln
195521	Ubuntu Security Notification for Json-c Vulnerabilities (USN-2245-1)	Vulnerability - level 4	Vuln
195573	Ubuntu Security Notification for Tomcat6, Tomcat7 Vulnerabilities (USN-2302-1)	Vulnerability - level 4	Vuln
195578	Ubuntu Security Notification for Openssl Vulnerabilities (USN-2308-1)	Vulnerability - level 4	Vuln
195599	Ubuntu Security Notification for Libreoffice Vulnerability (USN-2331-1)	Vulnerability - level 4	Vuln

195617	Ubuntu Security Notification for Dbus Vulnerabilities (USN-2352-1)	Vulnerability - level 4	Vuln
195661	Ubuntu Security Notification for Curl Vulnerability (USN-2399-1)	Vulnerability - level 4	Vuln
195662	Ubuntu Security Notification for Libreoffice Vulnerability (USN-2400-1)	Vulnerability - level 4	Vuln
195689	Ubuntu Security Notification for Libksba Vulnerability (USN-2427-1)	Vulnerability - level 4	Vuln
19569	Apache CouchDB Cross-Site Request Forgery Vulnerability	Potential Vulnerability - level 2	Practice
19569	WtCom Web Torrent SQL Injection Vulnerability	Potential Vulnerability - level 2	
195703	Ubuntu Security Notification for Linux Vulnerabilities (USN-2441-1)	Vulnerability - level 4	Vuln
195704	Ubuntu Security Notification for Linux-ec2 Vulnerabilities (USN-2442-1)	Vulnerability - level 4	Vuln
195705	Ubuntu Security Notification for Linux Vulnerabilities (USN-2443-1)	Vulnerability - level 4	Vuln
195706	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-2444-1)	Vulnerability - level 4	Vuln
195707	Ubuntu Security Notification for Linux-lts-trusty Vulnerabilities (USN-2445-1)	Vulnerability - level 4	Vuln
195708	Ubuntu Security Notification for Linux Vulnerabilities (USN-2446-1)	Vulnerability - level 4	Vuln
195709	Ubuntu Security Notification for Linux-lts-utopic Vulnerabilities (USN-2447-1)	Vulnerability - level 4	Vuln
195710	Ubuntu Security Notification for Linux Vulnerabilities (USN-2448-1)	Vulnerability - level 4	Vuln
19574	MambelFish Mambo Component Mambelfish.Class.PHP Remote File Include Vulnerability	Vulnerability - level 4	
19574	Oracle Database July 2009 Patch Set Update (PSU) 10.2.0.4.1 Not Installed (Patch 8576156)	Vulnerability - level 4	Vuln
195742	Ubuntu Security Notification for Tomcat6, Tomcat7 Vulnerabilities (USN-2130-1)	Vulnerability - level 4	Vuln
195755	Ubuntu Security Notification for Libssh Vulnerability (USN-2145-1)	Vulnerability - level 3	Vuln
195761	Ubuntu Security Notification for Linux Vulnerabilities (USN-2107-1)	Vulnerability - level 4	Vuln
195762	Ubuntu Security Notification for Linux-ec2 Vulnerabilities (USN-2108-1)	Vulnerability - level 4	Vuln
195774	Ubuntu Security Notification for Linux-lts-quantal Vulnerabilities (USN-2111-1)	Vulnerability - level 3	Vuln
195775	Ubuntu Security Notification for Linux-lts-raring Vulnerabilities (USN-2112-1)	Vulnerability - level 3	Vuln
195776	Ubuntu Security Notification for Linux Vulnerabilities (USN-2114-1)	Vulnerability - level 3	Vuln
195777	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-2115-1)	Vulnerability - level 3	Vuln
195778	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-2116-1)	Vulnerability - level 3	Vuln
195787	Ubuntu Security Notification for Openssl Vulnerabilities (USN-2459-1)	Vulnerability - level 4	Vuln
195789	Ubuntu Security Notification for Firefox Vulnerabilities (USN-2458-1)	Vulnerability - level 4	Vuln
195792	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-2464-1)	Vulnerability - level 4	Vuln
195810	Ubuntu Security Notification for Openssl Vulnerabilities (USN-2079-1)	Vulnerability - level 4	Vuln
195815	Ubuntu Security Notification for Devscripts Vulnerability (USN-2084-1)	Vulnerability - level 4	Vuln

195822	Ubuntu Security Notification for Gnupg Vulnerability (USN-2059-1)	Vulnerability - level 4	Vuln
195823	Ubuntu Security Notification for Libjpeg-turbo, Libjpeg6b Vulnerabilities (USN-2060-1)	Vulnerability - level 4	Vuln
195827	Ubuntu Security Notification for Linux Vulnerabilities (USN-2064-1)	Vulnerability - level 4	Vuln
195828	Ubuntu Security Notification for Linux-ec2 Vulnerabilities (USN-2065-1)	Vulnerability - level 4	Vuln
195829	Ubuntu Security Notification for Linux Vulnerabilities (USN-2066-1)	Vulnerability - level 4	Vuln
195830	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-2067-1)	Vulnerability - level 4	Vuln
195831	Ubuntu Security Notification for Linux-lts-quantal Vulnerabilities (USN-2068-1)	Vulnerability - level 4	Vuln
195832	Ubuntu Security Notification for Linux-lts-raring Vulnerabilities (USN-2069-1)	Vulnerability - level 4	Vuln
195833	Ubuntu Security Notification for Linux-lts-saucy Vulnerabilities (USN-2070-1)	Vulnerability - level 4	Vuln
195834	Ubuntu Security Notification for Linux Vulnerabilities (USN-2071-1)	Vulnerability - level 4	Vuln
195835	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-2072-1)	Vulnerability - level 4	Vuln
195836	Ubuntu Security Notification for Linux Vulnerabilities (USN-2073-1)	Vulnerability - level 4	Vuln
195837	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-2074-1)	Vulnerability - level 4	Vuln
195838	Ubuntu Security Notification for Linux Vulnerabilities (USN-2075-1)	Vulnerability - level 4	Vuln
195842	Ubuntu Security Notification for Jasper Vulnerabilities (USN-2483-1)	Vulnerability - level 4	Vuln
195843	Ubuntu Security Notification for Unbound Vulnerability (USN-2484-1)	Vulnerability - level 4	Vuln
195872	Ubuntu Security Notification for Firefox Vulnerabilities (USN-2031-1)	Vulnerability - level 4	Vuln
195873	Ubuntu Security Notification for Thunderbird Vulnerabilities (USN-2032-1)	Vulnerability - level 4	Vuln
19589	Coppermine Gallery Component for Mambo cpg.PHP Remote File Include Vulnerability	Vulnerability - level 5	
19589	Oracle Database October 2010 Security Update Multiple Vulnerabilities	Vulnerability - level 5	Practice
195893	Ubuntu Security Notification for Firefox Vulnerabilities (USN-2052-1)	Vulnerability - level 4	Vuln
195894	Ubuntu Security Notification for Thunderbird Vulnerabilities (USN-2053-1)	Vulnerability - level 4	Vuln
19592	Joomla Poll Component Multiple User Session Validation Vulnerability	Vulnerability - level 3	
19592	Oracle 11.2.0.1 on Microsoft Windows - General Update Multiple Issues (Patch #6)	Vulnerability - level 3	Vuln
195937	Ubuntu Security Notification for Nas Vulnerabilities (USN-1986-1)	Vulnerability - level 3	Vuln
195938	Ubuntu Security Notification for Gnupg, Gnupg2 Vulnerabilities (USN-1987-1)	Vulnerability - level 3	Vuln
195955	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-1942-1)	Vulnerability - level 4	Vuln
195973	Ubuntu Security Notification for Linux-lts-quantal Vulnerabilities (USN-1931-1)	Vulnerability - level 3	Vuln
195974	Ubuntu Security Notification for Linux Vulnerabilities (USN-1932-1)	Vulnerability - level 3	Vuln
195975	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-1933-1)	Vulnerability - level 3	Vuln

195976	Ubuntu Security Notification for Linux-ti-omap4 Vulnerabilities (USN-1934-1)	Vulnerability - level 3	Vuln
195979	Ubuntu Security Notification for Linux Vulnerabilities (USN-1912-1)	Vulnerability - level 3	Vuln
195980	Ubuntu Security Notification for Linux-ec2 Vulnerabilities (USN-1913-1)	Vulnerability - level 3	Vuln
195993	Ubuntu Security Notification for Raptor2 Vulnerability (USN-1901-1)	Vulnerability - level 3	Vuln
195994	Ubuntu Security Notification for Ruby1.8, Ruby1.9.1 Vulnerability (USN-1902-1)	Vulnerability - level 3	Vuln
195995	Ubuntu Security Notification for Apache2 Vulnerabilities (USN-1903-1)	Vulnerability - level 3	Vuln
195997	Ubuntu Security Notification for Ntp Vulnerabilities (USN-2497-1)	Vulnerability - level 3	Vuln
196003	Ubuntu Security Notification for Unzip Vulnerabilities (USN-2502-1)	Vulnerability - level 3	Vuln
196023	Ubuntu Security Notification for Icu Vulnerabilities (USN-2522-1)	Vulnerability - level 4	Vuln
196032	Ubuntu Security Notification for Openssl Vulnerabilities (USN-2537-1)	Vulnerability - level 4	Vuln
196056	Ubuntu Security Notification for Jakarta-taglibs-standard Vulnerability (USN-2551-1)	Vulnerability - level 3	Vuln
196068	Ubuntu Security Notification for Ntp Vulnerabilities (USN-2567-1)	Vulnerability - level 3	Vuln
196079	Ubuntu Security Notification for Wpa Vulnerability (USN-2577-1)	Vulnerability - level 3	Vuln
196142	Ubuntu Security Notification for Openssl Vulnerabilities (USN-2639-1)	Vulnerability - level 3	Vuln
196156	Ubuntu Security Notification for Tomcat7 Vulnerabilities (USN-2654-1)	Vulnerability - level 3	Vuln
196157	Ubuntu Security Notification for Tomcat6 Vulnerabilities (USN-2655-1)	Vulnerability - level 3	Vuln
196172	Ubuntu Security Notification for Firefox Vulnerabilities (USN-2656-1)	Vulnerability - level 3	Vuln
196176	Ubuntu Security Notification for Thunderbird Vulnerabilities (USN-2673-1)	Vulnerability - level 3	Vuln
196197	Ubuntu Security Notification for Openjdk-7 Vulnerabilities (USN-2696-1)	Vulnerability - level 3	Vuln
196203	Ubuntu Security Notification for Oxide-qt Vulnerabilities (USN-2677-1)	Vulnerability - level 3	Vuln
196207	Ubuntu Security Notification for Openjdk-6 Vulnerabilities (USN-2706-1)	Vulnerability - level 3	Vuln
196211	Ubuntu Security Notification for Openssh Vulnerabilities (USN-2710-1)	Vulnerability - level 3	Vuln
196221	Ubuntu Security Notification for Subversion Vulnerabilities (USN-2721-1)	Vulnerability - level 3	Vuln
196269	Ubuntu Security Notification for Commons-httpclient Vulnerabilities (USN-2769-1)	Vulnerability - level 3	Vuln
196284	Ubuntu Security Notification for Ntp Vulnerabilities (USN-2783-1)	Vulnerability - level 3	Vuln
196311	Ubuntu Security Notification for Krb5 Vulnerabilities (USN-2810-1)	Vulnerability - level 3	Vuln
196329	Ubuntu Security Notification for Openssl Vulnerabilities (USN-2830-1)	Vulnerability - level 3	Vuln
196383	Ubuntu Security Notification for Openssl Vulnerability (USN-2883-1)	Vulnerability - level 3	Vuln
196413	Ubuntu Security Notification for Openssl Vulnerabilities (USN-2914-1)	Vulnerability - level 4	Vuln
196424	Ubuntu Security Notification for Samba Vulnerabilities (USN-2922-1)	Vulnerability - level 3	Vuln
196457	Ubuntu Security Notification for Openssl Vulnerabilities (USN-2959-1)	Vulnerability - level 3	Vuln
196464	Ubuntu Security Notification for Openssh Vulnerabilities (USN-2966-1)	Vulnerability - level 3	Vuln

196522	Ubuntu Security Notification for Tomcat6, Tomcat7 Vulnerabilities (USN-3024-1)	Vulnerability - level 3	Vuln
196537	Ubuntu Security Notification for Apache2 Vulnerability (USN-3038-1)	Vulnerability - level 3	Vuln
196544	Ubuntu Security Notification for Php5, Php7.0 Vulnerabilities (USN-3045-1)	Vulnerability - level 3	Vuln
196547	Ubuntu Security Notification for Curl Vulnerabilities (USN-3048-1)	Vulnerability - level 3	Vuln
196552	Ubuntu Security Notification for Linux-lts-vivid Vulnerabilities (USN-3053-1)	Vulnerability - level 3	Vuln
196568	Ubuntu Security Notification for Linux Vulnerabilities (USN-3070-1)	Vulnerability - level 3	Vuln
196576	Ubuntu Security Notification for Webkit2gtk Vulnerabilities (USN-3079-1)	Vulnerability - level 3	Vuln
196585	Ubuntu Security Notification for Openssl Vulnerabilities (USN-3087-1)	Vulnerability - level 4	Vuln
196593	Ubuntu Security Notification for Ntp Vulnerabilities (USN-3096-1)	Vulnerability - level 3	Vuln
196621	Ubuntu Security Notification for Curl Vulnerabilities (USN-3123-1)	Vulnerability - level 3	Vuln
196629	Ubuntu Security Notification for Imagemagick Vulnerabilities (USN-3131-1)	Vulnerability - level 3	Vuln
19664	Linux Kernel Non-Hugemem Support Local Denial of Service Vulnerability	Vulnerability - level 4	
19664	Oracle Database April 2012 Security Update Multiple Vulnerabilities (CPUAPR2012)	Vulnerability - level 4	Practice
196672	Ubuntu Security Notification for Tomcat6, Tomcat7, Tomcat8 Vulnerabilities (USN-3177-1)	Vulnerability - level 3	Vuln
196677	Ubuntu Security Notification for Openssl Vulnerabilities (USN-3181-1)	Vulnerability - level 3	Vuln
196707	Ubuntu Security Notification for Tiff Vulnerabilities (USN-3212-1)	Vulnerability - level 3	Vuln
196728	Ubuntu Security Notification for Pidgin Vulnerability (USN-3231-1)	Vulnerability - level 3	Vuln
196745	Ubuntu Security Notification for Linux, Linux-ti-omap4 Vulnerability (USN-3248-1)	Vulnerability - level 3	Vuln
196746	Ubuntu Security Notification for Linux, Linux-aws, Linux-gke, Linux-raspi2, Linux-snapdragon Vulnerability (USN-3249-1)	Vulnerability - level 3	Vuln
196747	Ubuntu Security Notification for Linux Vulnerability (USN-3250-1)	Vulnerability - level 3	Vuln
196748	Ubuntu Security Notification for Linux, Linux-raspi2 Vulnerability (USN-3251-1)	Vulnerability - level 3	Vuln
196757	Ubuntu Security Notification for Qemu Vulnerabilities (USN-3261-1)	Vulnerability - level 3	Vuln
196764	Ubuntu Security Notification for Qemu Vulnerabilities (USN-3268-1)	Vulnerability - level 3	Vuln
196832	Ubuntu Security Notification for Openvpn Vulnerabilities (USN-3339-1)	Vulnerability - level 3	Vuln
19684	MySQL MyISAM Table Privilege Check Bypass Vulnerability	Potential Vulnerability - level 2	Practice
19684	NetBSD In-Kernel PPP Multiple Buffer Overflow Vulnerabilities	Potential Vulnerability - level 2	
196843	Ubuntu Security Notification for Ntp Vulnerabilities (USN-3349-1)	Vulnerability - level 3	Vuln
196860	Ubuntu Security Notification for Openjdk-8 Vulnerabilities (USN-3366-1)	Vulnerability - level 3	Vuln
196888	Ubuntu Security Notification for Openjdk-7 Vulnerabilities (USN-3396-1)	Vulnerability - level 3	Vuln
19690	MySQL Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
19690	Wireshark Multiple Vulnerabilities	Potential Vulnerability - level 4	

196932	Ubuntu Security Notification for Curl Vulnerabilities (USN-3441-1)	Vulnerability - level 3	Vuln
196947	Ubuntu Security Notification for Wpa Vulnerabilities (USN-3455-1) (KRACK Attack)	Vulnerability - level 4	Vuln
196952	Ubuntu Security Notification for Webkit2gtk Vulnerabilities (USN-3460-1)	Vulnerability - level 3	Vuln
196966	Ubuntu Security Notification for Openssl Vulnerabilities (USN-3475-1)	Vulnerability - level 3	Vuln
196995	Ubuntu Security Notification for Linux-firmware Vulnerabilities (USN-3505-1)	Vulnerability - level 3	Vuln
197002	Ubuntu Security Notification for Openssl Vulnerabilities (USN-3512-1)	Vulnerability - level 3	Vuln
197025	Ubuntu Security Notification for Openssh Vulnerabilities (USN-3538-1)	Vulnerability - level 3	Vuln
197059	Ubuntu Security Notification for Quagga Vulnerabilities (USN-3573-1)	Vulnerability - level 3	Vuln
197153	Ubuntu Security Notification for Tomcat7, Tomcat8 Vulnerabilities (USN-3665-1)	Vulnerability - level 3	Vuln
197180	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL1.0) Vulnerabilities (USN-3692-1)	Vulnerability - level 3	Vuln
197184	Ubuntu Security Notification for Linux, Linux-aws, Linux-kvm, Linux-raspi2, Linux-snapdragon Vulnerabilities (USN-3696-1)	Vulnerability - level 3	Vuln
197220	Ubuntu Security Notification for Linux, Linux-aws, Linux-azure, Linux-gcp, Linux-kvm, Linux-oem, (USN-3732-1)	Vulnerability - level 3	Vuln
197229	Ubuntu Security Notification for Linux, Linux-aws, Linux-kvm, Linux-raspi2, Linux-snapdragon Vulnerabilities (USN-3741-1)	Vulnerability - level 3	Vuln
197230	Ubuntu Security Notification for Linux Vulnerabilities (USN-3742-1)	Vulnerability - level 3	Vuln
197233	Ubuntu Security Notification for Wpa Vulnerability (USN-3745-1)	Vulnerability - level 3	Vuln
197242	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-3754-1)	Vulnerability - level 3	Vuln
197244	Ubuntu Security Notification for Intel-microcode Vulnerabilities (USN-3756-1)	Vulnerability - level 3	Vuln
197252	Ubuntu Security Notification for Curl Vulnerability (USN-3765-1)	Vulnerability - level 3	Vuln
197290	Ubuntu Security Notification for Curl Vulnerabilities (USN-3805-1)	Vulnerability - level 3	Vuln
197334	Ubuntu Security Notification for Nss Vulnerabilities (USN-3850-1)	Vulnerability - level 3	Vuln
197361	Ubuntu Security Notification for Libvncserver Vulnerabilities (USN-3877-1)	Vulnerability - level 4	Vuln
197382	Ubuntu Security Notification for Nss Vulnerability (USN-3898-1)	Vulnerability - level 3	Vuln
197429	Ubuntu Security Notification for Rssh Vulnerabilities (USN-3946-1)	Vulnerability - level 3	Vuln
197547	Ubuntu Security Notification for Ansible Vulnerabilities (USN-4072-1)	Vulnerability - level 3	Vuln
197557	Ubuntu Security Notification for Subversion Vulnerabilities (USN-4082-1)	Vulnerability - level 3	Vuln
197606	Ubuntu Security Notification for Python2.7, Python3.5, Python3.6, Python3.7 Vulnerabilities (USN-4127-1)	Vulnerability - level 3	Vuln
197717	Ubuntu Security Notification for Nss Vulnerability (USN-4203-1)	Vulnerability - level 3	Vuln
197719	Ubuntu Security Notification for Sqlite3 Vulnerabilities (USN-4205-1)	Vulnerability - level 3	Vuln
197730	Ubuntu Security Notification for Firefox Vulnerabilities (USN-4216-1)	Vulnerability - level 3	Vuln
197754	Ubuntu Security Notification for Thunderbird Vulnerabilities (USN-4241-1)	Vulnerability - level 3	Vuln
197791	Ubuntu Security Notification for Libxml2 Vulnerabilities (USN-4274-1)	Vulnerability - level 3	Vuln
197815	Ubuntu Security Notification for Sqlite3 Vulnerabilities (USN-4298-1)	Vulnerability - level 3	Vuln

19784	IBM DB2 Multiple Vulnerabilities (4963797,4964001,4964127,4963995,212611,212619,473453,477045)	Vulnerability - level 3	Vuln
19784	Lyris ListManager Unauthorized Administrative User Addition Vulnerability	Vulnerability - level 3	
197857	Ubuntu Security Notification for Thunderbird Vulnerabilities (USN-4335-1)	Vulnerability - level 3	Vuln
19788	Evision CMS Path Parameter Multiple Remote File Include Vulnerabilities	Vulnerability - level 4	
19788	Oracle Database October 2012 Security Update Multiple Vulnerabilities (CPUOCT2012)	Vulnerability - level 4	Practice
19789	Membypass Multiple Cross-Site Scripting Vulnerabilities	Vulnerability - level 4	
19789	Oracle Database October 2012 Patch Set Update (PSU) 11.2.0.3.4 Not Installed (Patch 14275605)	Vulnerability - level 4	Vuln
19790	Membypass Variable.PHP Remote File Include Vulnerability	Vulnerability - level 4	
19790	Oracle Database October 2012 Patch Set Update (PSU) 11.2.0.2.8 Not Installed (Patch 14275621)	Vulnerability - level 4	Vuln
197902	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-4376-1)	Vulnerability - level 3	Vuln
19791	Membypass Recherchemembre.php .PHP SQL Injection Vulnerability	Vulnerability - level 4	
19791	Oracle Database October 2012 Patch Set Update (PSU) 11.1.0.7.13 Not Installed (Patch 14275623)	Vulnerability - level 4	Vuln
197912	Ubuntu Security Notification for Intel-microcode Vulnerabilities (USN-4385- 1)	Vulnerability - level 3	Vuln
197914	Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-5.3, Linux- azure, Linux-azure-5.3, Linux-gcp, (USN-4387-1)	Vulnerability - level 3	Vuln
197915	Ubuntu Security Notification for Linux-gke-5.0, Linux-oem-osp1 Vulnerabilities (USN-4388-1)	Vulnerability - level 3	Vuln
197916	Ubuntu Security Notification for Linux, Linux-aws, Linux-azure, Linux-gcp, Linux-kvm, Linux-oracle (USN-4389-1)	Vulnerability - level 3	Vuln
197917	Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-hwe, Linux- azure, Linux-azure-4.15, Linux-gcp, (USN-4390-1)	Vulnerability - level 3	Vuln
197918	Ubuntu Security Notification for Linux, Linux-aws, Linux-kvm Vulnerabilities (USN-4391-1)	Vulnerability - level 3	Vuln
197919	Ubuntu Security Notification for Sqlite3 Vulnerabilities (USN-4394-1)	Vulnerability - level 3	Vuln
19792	Oracle Database October 2012 Patch Set Update (PSU)10.2.0.5.9 Not Installed (Patch 14275629)	Vulnerability - level 3	Vuln
197959	Ubuntu Security Notification for Libvncserver Vulnerabilities (USN-4434-1)	Vulnerability - level 3	Vuln
197967	Ubuntu Security Notification for Grub2 Vulnerability (USN-4432-1)	Vulnerability - level 4	Vuln
198025	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-4504-1)	Vulnerability - level 3	Vuln
198065	Ubuntu Security Notification for Libuv1 Vulnerability (USN-4548-1)	Vulnerability - level 3	Vuln
198066	Ubuntu Security Notification for Italc Vulnerabilities (USN-4547-1)	Vulnerability - level 3	Vuln
198091	Ubuntu Security Notification for Vino Vulnerabilities (USN-4573-1)	Vulnerability - level 3	Vuln
198113	Ubuntu Security Notification for Italc Vulnerabilities (USN-4587-1)	Vulnerability - level 3	Vuln
198143	Ubuntu Security Notification for Openldap Vulnerability (USN-4622-1)	Vulnerability - level 3	Vuln
198147	Ubuntu Security Notification for Linux, Linux-aws, Linux-azure, Linux-gcp, Linux-kvm, Linux-oracle, (USN-4626-1)	Vulnerability - level 3	Vuln
198148	Ubuntu Security Notification for Linux, Linux-gcp, Linux-gcp-4.15, Linux-gcp- 5.4, Linux-gke-4.15 (USN-4627-1)	Vulnerability - level 3	Vuln

198149	Ubuntu Security Notification for Intel-microcode Vulnerabilities (USN-4628-1)	Vulnerability - level 3	Vuln
198155	Ubuntu Security Notification for Openldap Vulnerabilities (USN-4634-1)	Vulnerability - level 3	Vuln
198179	Ubuntu Security Notification for Linux, Linux-aws, Linux-azure, Linux-kvm, Linux-lts-trusty, Linux-raspi2, (USN-4657-1)	Vulnerability - level 3	Vuln
198180	Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-5.4, Linux-azure, Linux-azure-5.4, Linux-gcp, (USN-4658-1)	Vulnerability - level 3	Vuln
198181	Ubuntu Security Notification for Linux, Linux-aws, Linux-azure, Linux-gcp, Linux-kvm, Linux-oracle, (USN-4659-1)	Vulnerability - level 3	Vuln
198184	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerability (USN-4662-1)	Vulnerability - level 3	Vuln
198187	Ubuntu Security Notification for Curl Vulnerabilities (USN-4665-1)	Vulnerability - level 3	Vuln
198197	Ubuntu Security Notification for LibVNCServer (USN-4407-1)	Vulnerability - level 3	Vuln
198206	Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-hwe, Linux-azure, Linux-azure-4.15, Linux-gcp, (USN-4680-1)	Vulnerability - level 3	Vuln
198218	Ubuntu Security Notification for Openvswitch Vulnerabilities (USN-4691-1)	Vulnerability - level 3	Vuln
198225	Ubuntu Security Notification for Dnsmasq Vulnerabilities (USN-4698-1)	Vulnerability - level 3	Vuln
19825	Oracle Database January 2013 Security Update Multiple Vulnerabilities (CPUJAN2013)	Vulnerability - level 4	Practice
19825	PHP-Nuke MyHeadlines Module Cross-Site Scripting Vulnerability	Vulnerability - level 4	
198253	Ubuntu Security Notification for Openldap Vulnerabilities (USN-4724-1)	Vulnerability - level 3	Vuln
19826	FlashChat Multiple Remote File Include Vulnerabilities	Vulnerability - level 4	
19826	Oracle Database January 2013 Patch Set Update (PSU) 11.2.0.3.5 Not Installed (Patch 14727310)	Vulnerability - level 4	Vuln
198267	Ubuntu Security Notification for Bind9 Vulnerability (USN-4737-1)	Vulnerability - level 3	Vuln
198268	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-4738-1)	Vulnerability - level 3	Vuln
19827	Oracle Database January 2013 Patch Set Update (PSU) 11.2.0.2.9 Not Installed (Patch 14727315)	Vulnerability - level 4	Vuln
19828	Oracle Database January 2013 Patch Set Update (PSU) 11.1.0.7.14 Not Installed (Patch 14739378)	Vulnerability - level 4	Vuln
19829	Oracle Database January 2013 Patch Set Update (PSU) 10.2.0.5.10 Not Installed (Patch 14727319)	Vulnerability - level 4	Vuln
19829	VTiger CRM HTML Injection and Access Control Bypass Vulnerabilities	Vulnerability - level 4	
19830	MyBace User_Daten.PHP Remote File Include Vulnerability	Vulnerability - level 4	
19830	Oracle Database January 2013 Patch Set Update (PSU) 10.2.0.4.15 Not Installed (Patch 14736542)	Vulnerability - level 4	Vuln
198310	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerability (USN-4891-1)	Vulnerability - level 3	Vuln
198348	Ubuntu Security Notification for Bind vulnerabilities (USN-4929-1)	Vulnerability - level 3	Vuln
198372	Ubuntu Security Notification for Intel Microcode vulnerabilities (USN-4628-3)	Vulnerability - level 2	Vuln
198391	Ubuntu Security Notification for PostgreSQL vulnerabilities (USN-4972-1)	Vulnerability - level 3	Vuln
198409	Ubuntu Security Notification for libxml2 vulnerabilities (USN-4991-1)	Vulnerability - level 4	Vuln
198410	Ubuntu Security Notification for GRUB 2 vulnerabilities (USN-4992-1)	Vulnerability - level 4	Vuln
198411	Ubuntu Security Notification for Intel Microcode vulnerabilities (USN-4985-1)	Vulnerability - level 3	Vuln

198413	Ubuntu Security Notification for Apache HTTP Server vulnerabilities (USN-4994-1)	Vulnerability - level 3	Vuln
198416	Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4997-1)	Vulnerability - level 4	Vuln
198417	Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4999-1)	Vulnerability - level 4	Vuln
198418	Ubuntu Security Notification for Linux kernel vulnerabilities (USN-5000-1)	Vulnerability - level 4	Vuln
198419	Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-5001-1)	Vulnerability - level 4	Vuln
198425	Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-5000-2)	Vulnerability - level 4	Vuln
198426	Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-4997-2)	Vulnerability - level 4	Vuln
198458	Ubuntu Security Notification for PostgreSQL vulnerabilities (USN-5038-1)	Vulnerability - level 2	Vuln
198459	Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-hwe, Linux-azure, Linux-azure-4.15, Linux-gcp, (USN-5018-1)	Vulnerability - level 3	Vuln
198469	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5051-1)	Vulnerability - level 3	Vuln
19847	PostgreSQL Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
19847	SoftBB Page Parameter Cross-Site Scripting Vulnerability	Potential Vulnerability - level 4	
198473	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerability (USN-5051-3)	Vulnerability - level 3	Vuln
198516	Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-5090-1)	Vulnerability - level 3	Vuln
198517	Ubuntu Security Notification for EDK II Vulnerabilities (USN-5088-1)	Vulnerability - level 3	Vuln
198525	Ubuntu Security Notification for docker.io Vulnerability (USN-5103-1)	Vulnerability - level 2	Vuln
198530	Ubuntu Security Notification for containerd Vulnerability (USN-5100-1)	Vulnerability - level 3	Vuln
198558	Ubuntu Security Notification for Bind Vulnerability (USN-5126-1)	Vulnerability - level 3	Vuln
198560	Ubuntu Security Notification for Docker Vulnerability (USN-5134-1)	Vulnerability - level 3	Vuln
198599	Ubuntu Security Notification for BusyBox Vulnerabilities (USN-5179-1)	Vulnerability - level 4	Vuln
198617	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5209-1)	Vulnerability - level 4	Vuln
198671	Ubuntu Security Notification for Expat Vulnerabilities (USN-5288-1)	Vulnerability - level 5	Vuln
19868	MySource Classic PHP Code Injection Vulnerability	Vulnerability - level 4	
19868	Oracle Database October 2013 Security Update Multiple Vulnerabilities (CPUOCT2013)	Vulnerability - level 4	Practice
19869	Oracle Database October 2013 Patch Set Update (PSU) 11.1.0.7.17 Not Installed (Patch 17082366)	Vulnerability - level 4	Vuln
198693	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5319-1)	Vulnerability - level 3	Vuln
198694	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5317-1)	Vulnerability - level 4	Vuln
198695	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5318-1)	Vulnerability - level 4	Vuln
198697	Ubuntu Security Notification for libxml2 Vulnerability (USN-5324-1)	Vulnerability - level 4	Vuln
19870	Akaru Social BookMarking Engine Main_Content.PHP Remote File Include Vulnerability	Vulnerability - level 4	

19870	Oracle Database October 2013 Patch Set Update (PSU) 11.2.0.2.12 Not Installed (Patch 17082367)	Vulnerability - level 4	Vuln
198705	Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-5333-1)	Vulnerability - level 4	Vuln
198706	Ubuntu Security Notification for Bind Vulnerabilities (USN-5332-1)	Vulnerability - level 4	Vuln
198713	Ubuntu Security Notification for Open Virtual Private Network (OpenVPN) Vulnerability (USN-5347-1)	Vulnerability - level 4	Vuln
19872	Oracle Database October 2013 Patch Set Update (PSU) 11.2.0.3.8 Not Installed (Patch 16902043)	Vulnerability - level 4	Vuln
19872	Php Download Download.PHP Directory Traversal Vulnerability	Vulnerability - level 4	
198728	Ubuntu Security Notification for Linux kernel (Intel IOTG) Vulnerabilities (USN-5362-1)	Vulnerability - level 4	Vuln
19873	Beautifier Core.PHP Remote File Include Vulnerability	Vulnerability - level 4	
19873	Oracle Database October 2013 Patch Set Update (PSU) 12.1.0.1.1 Not Installed (Patch 17027533)	Vulnerability - level 4	Practice
198747	Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5381-1)	Vulnerability - level 4	Vuln
198767	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5390-1)	Vulnerability - level 4	Vuln
198770	Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5390-2)	Vulnerability - level 4	Vuln
198771	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5402-1)	Vulnerability - level 4	Vuln
198782	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5417-1)	Vulnerability - level 4	Vuln
198783	Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5416-1)	Vulnerability - level 4	Vuln
198784	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5418-1)	Vulnerability - level 4	Vuln
198785	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5415-1)	Vulnerability - level 4	Vuln
198787	Ubuntu Security Notification for libxml2 Vulnerabilities (USN-5422-1)	Vulnerability - level 4	Vuln
198804	Ubuntu Security Notification for Subversion Vulnerabilities (USN-5445-1)	Vulnerability - level 4	Vuln
198819	Ubuntu Security Notification for E2fsprogs Vulnerability (USN-5464-1)	Vulnerability - level 4	Vuln
198822	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5469-1)	Vulnerability - level 4	Vuln
198824	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5467-1)	Vulnerability - level 4	Vuln
198825	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5466-1)	Vulnerability - level 4	Vuln
198826	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5468-1)	Vulnerability - level 4	Vuln
198838	Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-5487-1)	Vulnerability - level 5	Vuln
198839	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerability (USN-5488-1)	Vulnerability - level 4	Vuln
198850	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerability (USN-5502-1)	Vulnerability - level 4	Vuln
198857	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5514-1)	Vulnerability - level 3	Vuln
198858	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5515-1)	Vulnerability - level 4	Vuln
198861	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5518-1)	Vulnerability - level 4	Vuln

198875	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5539-1)	Vulnerability - level 4	Vuln
198891	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5560-1)	Vulnerability - level 4	Vuln
198895	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5562-1)	Vulnerability - level 4	Vuln
198897	Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5564-1)	Vulnerability - level 4	Vuln
198911	Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-5582-1)	Vulnerability - level 4	Vuln
198921	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5594-1)	Vulnerability - level 5	Vuln
198927	Ubuntu Security Notification for Linux kernel (Oracle) Vulnerabilities (USN-5599-1)	Vulnerability - level 5	Vuln
198929	Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5602-1)	Vulnerability - level 5	Vuln
198942	Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5616-1)	Vulnerability - level 5	Vuln
198943	Ubuntu Security Notification for Xen Vulnerabilities (USN-5617-1)	Vulnerability - level 4	Vuln
198949	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5622-1)	Vulnerability - level 5	Vuln
198950	Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-5623-1)	Vulnerability - level 5	Vuln
198954	Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5630-1)	Vulnerability - level 5	Vuln
198962	Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-5639-1)	Vulnerability - level 5	Vuln
198966	Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5647-1)	Vulnerability - level 5	Vuln
198970	Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5654-1)	Vulnerability - level 4	Vuln
198974	Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5660-1)	Vulnerability - level 4	Vuln
198978	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5669-1)	Vulnerability - level 4	Vuln
198979	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5667-1)	Vulnerability - level 4	Vuln
198980	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5668-1)	Vulnerability - level 4	Vuln
198985	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5678-1)	Vulnerability - level 4	Vuln
198987	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5677-1)	Vulnerability - level 4	Vuln
198989	Ubuntu Security Notification for Linux kernel (IBM) Vulnerabilities (USN-5683-1)	Vulnerability - level 4	Vuln
198990	Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-5682-1)	Vulnerability - level 4	Vuln
198994	Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5687-1)	Vulnerability - level 4	Vuln
199009	Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5703-1)	Vulnerability - level 4	Vuln
199011	Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-5706-1)	Vulnerability - level 4	Vuln
199030	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5727-1)	Vulnerability - level 4	Vuln
199036	Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5727-2)	Vulnerability - level 4	Vuln
199072	Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5774-1)	Vulnerability - level 4	Vuln

199150	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5844-1)	Vulnerability - level 4	Vuln
199151	Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5845-1)	Vulnerability - level 4	Vuln
199210	Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5913-1)	Vulnerability - level 4	Vuln
199268	Ubuntu Security Notification for Samba Vulnerabilities (USN-5993-1)	Vulnerability - level 4	Vuln
199270	Ubuntu Security Notification for Idb Vulnerability (USN-5992-1)	Vulnerability - level 4	Vuln
199397	Ubuntu Security Notification for nghhttp2 Vulnerability (USN-6142-1)	Vulnerability - level 4	Vuln
19949	MiniPortal Menu.PHP Remote File Include Vulnerability	Potential Vulnerability - level 4	
19949	Oracle MySQL October 2014 Critical Patch Update	Potential Vulnerability - level 4	Practice
19970	Oracle MySQL April 2015 Critical Patch Update (CPUAPR2015)	Potential Vulnerability - level 3	Practice
19985	ColdFusion SandBox Security Bypass Vulnerability	Vulnerability - level 4	
19985	IBM DB2 General Parallel File System Multiple Vulnerabilities (264025)	Vulnerability - level 4	Vuln
19986	IBM DB2 Multiple Vulnerabilities (4681455,4684449,264025,4688295,4690065,4690143,4906179,4906617,4676679,519777,4672917)	Vulnerability - level 4	Vuln
19986	Symantec AntiVirus Corporate Edition Multiple Local Format String Vulnerabilities	Vulnerability - level 4	
20004	Oracle MySQL April 2016 Critical Patch Update (CPUAPR2016)	Potential Vulnerability - level 5	Practice
20004	Snitz Forums 2000 Forum.ASP Cross-Site Scripting Vulnerability	Potential Vulnerability - level 5	
20020	ActiveCampaign KnowledgeBuilder Remote File Include Vulnerability	Potential Vulnerability - level 5	
20020	Oracle MySQL July 2016 Critical Patch Update (CPUJUL2016)	Potential Vulnerability - level 5	Practice
20063	Aceboard Recherche.PHP Cross-Site Scripting Vulnerability	Vulnerability - level 4	
20063	Oracle MySQL January 2018 Critical Patch Update (CPUJAN2018)	Vulnerability - level 4	Practice
20151	Oracle MySQL April 2020 Critical Patch Update (CPUAPR2020)	Vulnerability - level 4	Practice
20151	Simple HTTP Scanner Multiple Unspecified Vulnerabilities	Vulnerability - level 4	
20189	EvoBB Path Parameter Multiple Remote File Include Vulnerabilities	Vulnerability - level 5	
20189	Oracle Database 19c Critical Patch Update - October 2020	Vulnerability - level 5	Vuln
20190	IBM AIX CFGMGR Local Privilege Escalation and Arbitrary File Overwrite Vulnerabilities	Vulnerability - level 5	
20190	Oracle Database 18c Critical Patch Update - October 2020	Vulnerability - level 5	Vuln
20191	IBM AIX Slip.Login Local Privilege Escalation Vulnerability	Vulnerability - level 5	
20191	Oracle Database 12.2.0.1 Critical Patch Update - October 2020	Vulnerability - level 5	Vuln
20192	BrudaNews/GrudaGB Index.PHP Remote File Include Vulnerability	Potential Vulnerability - level 5	
20192	Oracle Database 12.2.0.1 Critical Patch Update - October 2020 (Unauthenticated)	Potential Vulnerability - level 5	Practice
20193	IBM Snappd AIX Local Arbitrary Command Execution Vulnerability	Vulnerability - level 5	
20193	Oracle Database 12.1.0.2 Critical Patch Update - October 2020	Vulnerability - level 5	Vuln
20194	IBM AIX RDIST Local Arbitrary File Overwrite Vulnerability	Potential Vulnerability - level 5	
20194	Oracle Database 12.1.0.2 Critical Patch Update - October 2020 (Unauthenticated)	Potential Vulnerability - level 5	Practice
20195	Oracle Database 11.2.0.4 Critical Patch Update - October 2020	Vulnerability - level 5	Vuln
20195	Sun Solaris 10 Malformed IPV6 Packets Denial of Service Vulnerability	Vulnerability - level 5	

20196	IBM AIX UUCP Local Privilege Escalation Vulnerability	Potential Vulnerability - level 5	
20196	Oracle Database 11.2.0.4 Critical Patch Update - October 2020 (Unauthenticated)	Potential Vulnerability - level 5	Practice
20221	Oracle MySQL April 2021 Critical Patch Update (CPUAPR2021)	Vulnerability - level 3	Practice
20221	PHP Invoice Home.PHP Cross-Site Scripting Vulnerability	Vulnerability - level 3	
20236	Oracle MySQL October 2021 Critical Patch Update (CPUOCT2021)	Vulnerability - level 4	Practice
20236	VirtueMart Joomla ECommerce Edition Multiple Input Validation Vulnerabilities	Vulnerability - level 4	
20253	Oracle Database 12.1.0.2 Critical Patch Update - April 2022	Vulnerability - level 5	Vuln
20253	PHPMyAdmin Multiple Unspecified Vulnerabilities	Vulnerability - level 5	
20254	FacileForms Unspecified Cross-Site Scripting Vulnerability	Potential Vulnerability - level 5	
20254	Oracle Database 12.1.0.2 Critical Patch Update - April 2022 (Unauthenticated)	Potential Vulnerability - level 5	Practice
20255	Oracle Database 19c Critical Patch Update - April 2022	Vulnerability - level 5	Vuln
20255	PPA Gallery Functions_Inc.PHP Remote File Include Vulnerability	Vulnerability - level 5	
20258	IBM DB2 Arbitrary Code Execution Vulnerability (6573293)	Vulnerability - level 4	Vuln
20258	KGB Kgcalls.php Local File Include Vulnerability	Vulnerability - level 4	
20259	IBM DB2 Multiple Vulnerabilities (6597637)	Vulnerability - level 4	Vuln
20259	Les Visiteurs Config.Inc.PHP Remote File Include Vulnerability	Vulnerability - level 4	
20266	Oracle MySQL July 2022 Critical Patch Update (CPUJUL2022)	Vulnerability - level 4	Practice
20266	UBB.threads Multiple Input Validation Vulnerabilities	Vulnerability - level 4	
20273	ConPresso CMS Multiple Input Validation Vulnerabilities	Vulnerability - level 3	
20273	Oracle MySQL October 2022 Critical Patch Update (CPUOCT2022)	Vulnerability - level 3	Practice
20285	Oracle Database 19c Critical OJVM Patch Update - April 2022	Vulnerability - level 5	Vuln
20288	McAfee EPolicy Orchestrator and ProtectionPilot HTTP Server Remote Buffer Overflow Vulnerability	Vulnerability - level 4	
20288	Oracle Database 19c Critical OJVM Patch Update - October 2020	Vulnerability - level 4	Vuln
20297	Digishop Cart.PHP Cross-Site Scripting Vulnerability	Vulnerability - level 4	
20297	Oracle Database 18c Critical OJVM Patch Update - October 2020	Vulnerability - level 4	Vuln
20313	Net2FTP Index.PHP Cross-Site Scripting Vulnerability	Vulnerability - level 4	
20313	Oracle Database 12.2.0.1 Critical OJVM Patch Update - October 2020	Vulnerability - level 4	Vuln
20344	Microsoft Excel DATETIME Remote Code Execution Vulnerability	Vulnerability - level 3	
20344	Oracle MySQL April 2023 Critical Patch Update (CPUAPR2023)	Vulnerability - level 3	Practice
216002	VMWare ESXi 5.0.0 Update 1 Missing (KB2010823)	Vulnerability - level 4	Vuln
216003	VMWare ESXi 5.0.0 Patch Release ESXi500-201112001 Missing (KB2007680)	Vulnerability - level 4	Vuln
216006	VMWare ESXi 4.1.0 Patch ESXi410-Update02 Missing (KB2002338)	Vulnerability - level 4	Vuln
216007	VMWare ESXi 4.1.0 Patch Release ESXi410-201104001 Missing (KB1035111)	Vulnerability - level 3	Vuln
216009	VMWare ESXi 4.1.0 Patch ESXi410-Update01 Missing (KB1029354)	Vulnerability - level 4	Vuln
216010	VMWare ESXi 4.1.0 Patch Release ESXi410-201010001 Missing (KB1027753)	Vulnerability - level 4	Vuln
216011	VMWare ESXi 4.0.0 Patch Release ESXi400-201110001 Missing (KB1036397)	Vulnerability - level 4	Vuln
216012	VMWare ESXi 4.0.0 Patch Release ESXi400-201104001 Missing (KB1037261)	Vulnerability - level 3	Vuln
216013	VMWare ESXi 4.0.0 Patch Release ESXi400-201103001 Missing (KB1032823)	Vulnerability - level 4	Vuln
216025	VMware ESX 4.0 Service Console Update for krb5 (VMSA-2009-0008)	Vulnerability - level 4	Vuln
216026	VMware ESX 4.0 Update for Multiple Packages (VMSA-2009-0016)	Vulnerability - level 4	Vuln
216027	VMware ESX 4.0 Third Party Updates for Service Console (VMSA-2010-0013)	Vulnerability - level 4	Vuln
216028	VMware ESX 4.x Third Party Updates for Service Console (VMSA-2010-0019)	Vulnerability - level 3	Vuln

216036	VMware ESXi and ESX Third Party Libraries Updates (VMSA-2012-0013)	Vulnerability - level 4	Vuln
216037	VMware Third Party Component Updates for ESX 4.x (VMSA-2011-0013)	Vulnerability - level 4	Vuln
216041	VMWare ESXi 5.0.0 Patch ESXi500-Update02 Missing (KB2033751)	Vulnerability - level 4	Vuln
216044	VMWare ESX 4.1.0 Patch Release ESX410-201301001 Missing (KB2041331)	Vulnerability - level 4	Vuln
216049	VMWare ESXi 5.1.0 Patch Complete Update 1 Missing (KB2041632)	Vulnerability - level 4	Vuln
216056	VMware ESXi 5.0.0 Patch ESXi500-Update03 Missing (KB2055559)	Vulnerability - level 3	Vuln
216061	VMware ESX 4.0.0 Patch Release ESX400-201310001 Missing (KB2059495)	Vulnerability - level 4	Vuln
216062	VMware ESXi 4.0.0 Patch Release ESXi400-201310001 Missing (KB2059496)	Vulnerability - level 4	Vuln
216063	VMware ESXi 5.1.0 Patch Complete Update 2 Missing (KB2062314)	Vulnerability - level 3	Vuln
216071	VMware ESXi 5.5.0 Patch Release ESXi550-201406001 Missing (KB2077359)	Vulnerability - level 4	Vuln
216072	VMware ESXi 5.1.0 Patch Release ESXi510-201406001 (KB2077640)	Vulnerability - level 4	Vuln
216076	VMware ESXi 5.1.0 Patch Complete Update 3 Missing (KB2086278)	Vulnerability - level 4	Vuln
216080	VMware ESXi 3.5 Patch Release ESXe350-201302401-I-SG Missing (KB2042543)	Vulnerability - level 5	Vuln
216089	VMware ESXi 3.5 Patch Release ESXe350-201203401-I-SG Missing (KB2009160)	Vulnerability - level 4	Vuln
216108	VMware ESXi 3.5 Patch Release ESX350-200912401-BG Missing (KB1016657)	Vulnerability - level 4	Vuln
216220	VMware security updates for vCenter Server (VMSA-2013-0006)	Vulnerability - level 4	Vuln
236003	Red Hat Update for openssh (RHSA-2016:0741)	Vulnerability - level 3	Vuln
236006	Red Hat Update for ntp (RHSA-2016:0780)	Vulnerability - level 3	Vuln
236016	Red Hat Update for openssl (RHSA-2016:1137)	Vulnerability - level 4	Vuln
236020	Red Hat Update for ntp (RHSA-2016:1141)	Vulnerability - level 3	Vuln
236041	Red Hat Update for flash-plugin (RHSA-2016:1423)	Vulnerability - level 5	Vuln
236042	Red Hat Update for httpd (RHSA-2016:1422) (HTTPoxy)	Vulnerability - level 4	Vuln
236043	Red Hat Update for httpd (RHSA-2016:1421) (HTTPoxy)	Vulnerability - level 4	Vuln
236064	Red Hat Update for ntp (RHSA-2016:1552)	Vulnerability - level 3	Vuln
236072	Red Hat Update for php (RHSA-2016:1613)	Vulnerability - level 3	Vuln
236074	Red Hat Update for php (RHSA-2016:1609)	Vulnerability - level 3	Vuln
236095	Red Hat Update for openssl security (RHSA-2016:1940)	Vulnerability - level 4	Vuln
236111	Red Hat Update for tomcat6 (RHSA-2016:2045)	Vulnerability - level 4	Vuln
236112	Red Hat Update for tomcat (RHSA-2016:2046)	Vulnerability - level 4	Vuln
236116	Red Hat Update for openssl (RHSA-2016:2073)	Vulnerability - level 4	Vuln
236143	Red Hat Update for curl (RHSA-2016:2575)	Vulnerability - level 3	Vuln
236146	Red Hat Update for ntp security (RHSA-2016:2583)	Vulnerability - level 3	Vuln
236157	Red Hat Update for openssh (RHSA-2016:2588)	Vulnerability - level 3	Vuln
236168	Red Hat Update for tomcat (RHSA-2016:2599)	Vulnerability - level 3	Vuln
236256	Red Hat Update for ntp security (RHSA-2017:0252)	Vulnerability - level 3	Vuln
236301	Red Hat Update for openssh Security (RHSA-2017:0641)	Vulnerability - level 3	Vuln
236396	Red Hat Update for java-1.8.0-openjdk (RHSA-2017:1789)	Vulnerability - level 5	Vuln
236397	Red Hat Update for java-1.8.0-oracle (RHSA-2017:1790)	Vulnerability - level 5	Vuln
236398	Red Hat Update for java-1.7.0-oracle (RHSA-2017:1791)	Vulnerability - level 5	Vuln
236399	Red Hat Update for Java (RHSA-2017:1792)	Vulnerability - level 5	Vuln
236422	Red Hat Update for curl (RHSA-2017:2016)	Vulnerability - level 3	Vuln
236426	Red Hat Update for openssh (RHSA-2017:2029)	Vulnerability - level 3	Vuln
236432	Red Hat Update for pidgin (RHSA-2017:1854)	Vulnerability - level 3	Vuln
236446	Red Hat Update for java-1.7.0-openjdk (RHSA-2017:2424)	Vulnerability - level 5	Vuln
236454	Red Hat Update for java-1.8.0-ibm (RHSA-2017:2469)	Vulnerability - level 5	Vuln
236459	Red Hat Update for java-1.7.1-ibm (RHSA-2017:2481)	Vulnerability - level 5	Vuln
236464	Red Hat Update for mercurial (RHSA-2017:2489)	Vulnerability - level 4	Vuln
236472	Red Hat Update for java-1.6.0-ibm (RHSA-2017:2530)	Vulnerability - level 5	Vuln
236530	Red Hat Update for wpa_supplicant (RHSA-2017:2907)	Vulnerability - level 4	Vuln
236531	Red Hat Update for wpa_supplicant (RHSA-2017:2911)	Vulnerability - level 4	Vuln

236532	Red Hat Update for kernel (RHSA-2017:2930)	Vulnerability - level 4	Vuln
236574	Red Hat Update for java-1.7.0-openjdk (RHSA-2017:3392)	Vulnerability - level 4	Vuln
236652	Red Hat Update for quagga (RHSA-2018:0377)	Vulnerability - level 4	Vuln
236712	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2018:0998)	Vulnerability - level 3	Vuln
236714	Red Hat Update for openssh (RHSA-2018:0980)	Vulnerability - level 2	Vuln
236907	Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.29 RHEL 7 (RHSA-2018:2185)	Vulnerability - level 3	Vuln
236908	Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.29 RHEL 6 (RHSA-2018:2186)	Vulnerability - level 3	Vuln
236928	Red Hat Update for kernel (RHSA-2018:2384)	Vulnerability - level 4	Vuln
236949	Red Hat Update for java-1.8.0-ibm (RHSA-2018:2568)	Vulnerability - level 4	Vuln
236953	Red Hat Update for java-1.8.0-ibm (RHSA-2018:2575)	Vulnerability - level 4	Vuln
236959	Red Hat Update for kernel (RHSA-2018:2645)	Vulnerability - level 4	Vuln
236966	Red Hat Update for kernel (RHSA-2018:2790)	Vulnerability - level 4	Vuln
236967	Red Hat Update for kernel (RHSA-2018:2785)	Vulnerability - level 4	Vuln
236968	Red Hat Update for kernel (RHSA-2018:2776)	Vulnerability - level 4	Vuln
237017	Red Hat Update for wpa_supplicant (RHSA-2018:3107)	Vulnerability - level 3	Vuln
237021	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2018:3221)	Vulnerability - level 3	Vuln
237033	Red Hat Update for xerces-c (RHSA-2018:3335)	Vulnerability - level 3	Vuln
237034	Red Hat Update for kernel-alt (RHSA-2018:2948)	Vulnerability - level 4	Vuln
237045	Red Hat Update for xerces-c (RHSA-2018:3506)	Vulnerability - level 3	Vuln
237047	Red Hat Update for xerces-c (RHSA-2018:3514)	Vulnerability - level 3	Vuln
237169	Red Hat Update for python (RHSA-2019:0710)	Vulnerability - level 4	Vuln
237192	Red Hat Update for python3 (RHSA-2019:0997)	Vulnerability - level 4	Vuln
237196	Red Hat Update for python27:2.7 (RHSA-2019:0981)	Vulnerability - level 4	Vuln
237270	Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.29 SP2 (RHSA-2019:1297)	Vulnerability - level 4	Vuln
237288	Red Hat Update for python (RHSA-2019:1467)	Vulnerability - level 4	Vuln
237342	Red Hat Update for json-c (RHSA-2014:0703)	Vulnerability - level 3	Vuln
237346	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2014:0679)	Vulnerability - level 4	Vuln
237391	Red Hat Update for nss and nspr (RHSA-2019:1951)	Vulnerability - level 3	Vuln
237395	Red Hat Update for curl (RHSA-2019:1880)	Vulnerability - level 2	Vuln
237411	Red Hat Update for nss, nss-softokn, nss-util, and nspr (RHSA-2019:2237)	Vulnerability - level 3	Vuln
237430	Red Hat Update for curl (RHSA-2019:2181)	Vulnerability - level 2	Vuln
237439	Red Hat Update for tomcat (RHSA-2019:2205)	Vulnerability - level 3	Vuln
237481	Red Hat Update for rh-python36-python (RHSA-2019:0765)	Vulnerability - level 4	Vuln
237484	Red Hat Update for python27-python (RHSA-2019:0806)	Vulnerability - level 4	Vuln
237487	Red Hat Update for rh-python35-python (RHSA-2019:0902)	Vulnerability - level 4	Vuln
237499	Red Hat Update for pki-deps:10.6 (RHSA-2019:1529)	Vulnerability - level 4	Vuln
237507	Red Hat Update for httpd24 (RHSA-2018:3558)	Vulnerability - level 3	Vuln
237514	Red Hat Update for subversion:1.10 (RHSA-2019:2512)	Vulnerability - level 4	Vuln
237678	Red Hat Update for python (RHSA-2019:2980)	Vulnerability - level 4	Vuln
237850	Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.23 Release on RHEL 6(RHSA-2017:0193)	Vulnerability - level 4	Vuln
237851	Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.23 Release on RHEL 7(RHSA-2017:0194)	Vulnerability - level 4	Vuln
237853	Red Hat Update for nss (RHSA-2019:4114)	Vulnerability - level 4	Vuln
237857	Red Hat Update for nss-softokn (RHSA-2019:4152)	Vulnerability - level 4	Vuln
237861	Red Hat Update for nss, nss-softokn, nss-util (RHSA-2019:4190)	Vulnerability - level 4	Vuln
237939	Red Hat Update for nss (RHSA-2020:0243)	Vulnerability - level 4	Vuln
237982	Red Hat Update for chromium-browser (RHSA-2020:0514)	Vulnerability - level 4	Vuln
238072	Red Hat Update for libvncserver (RHSA-2020:0920)	Vulnerability - level 4	Vuln
238076	Red Hat Update for libvncserver (RHSA-2020:0913)	Vulnerability - level 4	Vuln
238123	Red Hat Update for nss-softokn (RHSA-2020:1267)	Vulnerability - level 4	Vuln

238154	Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 SP2 (RHSA-2020:1337)	Vulnerability - level 3	Vuln
238159	Red Hat Update for python-XStatic-jQuery (RHSA-2020:1325)	Vulnerability - level 3	Vuln
238191	Red Hat Update for nss-softoken (RHSA-2020:1461)	Vulnerability - level 4	Vuln
238226	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2020:1840)	Vulnerability - level 3	Vuln
238228	Red Hat Update for sqlite (RHSA-2020:1810)	Vulnerability - level 3	Vuln
238310	Red Hat Update for libreswan (RHSA-2020:2071)	Vulnerability - level 4	Vuln
238311	Red Hat Update for libreswan (RHSA-2020:2070)	Vulnerability - level 4	Vuln
238359	Red Hat Update for microcode_ctl (RHSA-2020:2433)	Vulnerability - level 3	Vuln
238360	Red Hat Update for microcode_ctl (RHSA-2020:2432)	Vulnerability - level 3	Vuln
238361	Red Hat Update for microcode_ctl (RHSA-2020:2431)	Vulnerability - level 3	Vuln
238389	Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 SP3 (RHSA-2020:2644)	Vulnerability - level 4	Vuln
238410	Red Hat Update for microcode_ctl (RHSA-2020:2677)	Vulnerability - level 3	Vuln
238421	Red Hat Update for microcode_ctl (RHSA-2020:2758)	Vulnerability - level 3	Vuln
238425	Red Hat Update for httpd24-nghttp2 (RHSA-2020:2784)	Vulnerability - level 4	Vuln
238431	Red Hat Update for nghttp2 (RHSA-2020:2755)	Vulnerability - level 4	Vuln
238441	Red Hat Update for nodejs:12 (RHSA-2020:2852)	Vulnerability - level 4	Vuln
238443	Red Hat Update for nodejs:10 (RHSA-2020:2849)	Vulnerability - level 4	Vuln
238444	Red Hat Update for nodejs:10 (RHSA-2020:2848)	Vulnerability - level 4	Vuln
238445	Red Hat Update for nodejs:12 (RHSA-2020:2847)	Vulnerability - level 4	Vuln
238457	Red Hat Update for nghttp2 (RHSA-2020:2823)	Vulnerability - level 4	Vuln
238465	Red Hat Update for rh-nodejs12-nodejs (RHSA-2020:2895)	Vulnerability - level 4	Vuln
238469	Red Hat Update for microcode_ctl (RHSA-2020:2842)	Vulnerability - level 3	Vuln
238486	Red Hat Update for rh-nodejs10-nodejs (RHSA-2020:3084)	Vulnerability - level 4	Vuln
238511	Red Hat Update for grub2 (RHSA-2020:3223)	Vulnerability - level 4	Vuln
238517	Red Hat Update for grub2 (RHSA-2020:3217)	Vulnerability - level 4	Vuln
238518	Red Hat Update for grub2 (RHSA-2020:3216)	Vulnerability - level 4	Vuln
238522	Red Hat Update for libvncserver (RHSA-2020:3281)	Vulnerability - level 4	Vuln
238524	Red Hat Update for grub2 (RHSA-2020:3271)	Vulnerability - level 3	Vuln
238540	Red Hat Update for libvncserver (RHSA-2020:3385)	Vulnerability - level 4	Vuln
238548	Red Hat Update for grub2 (RHSA-2020:3274)	Vulnerability - level 3	Vuln
238555	Red Hat Update for libvncserver (RHSA-2020:3456)	Vulnerability - level 4	Vuln
238657	Red Hat Update for libxml2 (RHSA-2020:3996)	Vulnerability - level 3	Vuln
238662	Red Hat Update for subversion (RHSA-2020:3972)	Vulnerability - level 3	Vuln
238668	Red Hat Update for ipa (RHSA-2020:3936)	Vulnerability - level 3	Vuln
238726	Red Hat Update for nodejs:12 (RHSA-2020:4272)	Vulnerability - level 3	Vuln
238762	Red Hat Update for nodejs:12 (RHSA-2020:4903)	Vulnerability - level 3	Vuln
238764	Red Hat Update for pki-core:10.6 and pki-deps:10.6 (RHSA-2020:4847)	Vulnerability - level 3	Vuln
238776	Red Hat Update for subversion:1.10 (RHSA-2020:4712)	Vulnerability - level 3	Vuln
238802	Red Hat Update for libxml2 (RHSA-2020:4479)	Vulnerability - level 3	Vuln
238811	Red Hat Update for sqlite (RHSA-2020:4442)	Vulnerability - level 3	Vuln
238824	Red Hat Update for idm:DL1 and idm:client (RHSA-2020:4670)	Vulnerability - level 3	Vuln
238871	Red Hat Update for rh-nodejs12-nodejs (RHSA-2020:5086)	Vulnerability - level 3	Vuln
238872	Red Hat Update for microcode_ctl (RHSA-2020:5085)	Vulnerability - level 3	Vuln
238873	Red Hat Update for microcode_ctl (RHSA-2020:5084)	Vulnerability - level 3	Vuln
238874	Red Hat Update for microcode_ctl (RHSA-2020:5083)	Vulnerability - level 3	Vuln
238880	Red Hat Update for microcode_ctl (RHSA-2020:5190)	Vulnerability - level 3	Vuln
238881	Red Hat Update for microcode_ctl (RHSA-2020:5185)	Vulnerability - level 3	Vuln
238883	Red Hat Update for microcode_ctl (RHSA-2020:5181)	Vulnerability - level 3	Vuln
238911	Red Hat Update for microcode_ctl (RHSA-2020:5369)	Vulnerability - level 3	Vuln
238917	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2020:5566)	Vulnerability - level 4	Vuln
238932	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2020:5476)	Vulnerability - level 4	Vuln
238941	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2020:5422)	Vulnerability - level 4	Vuln

238961	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2020:5642)	Vulnerability - level 4	Vuln
238962	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2020:5637)	Vulnerability - level 4	Vuln
238964	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2020:5623)	Vulnerability - level 4	Vuln
238969	Red Hat Update for OpenShift Container Platform 4.6.9 packages (RHSA-2020:5615)	Vulnerability - level 4	Vuln
238973	Red Hat Update for python-XStatic-jQuery (RHSA-2020:5581)	Vulnerability - level 3	Vuln
238975	Red Hat Update for python-XStatic-Bootstrap-SCSS (RHSA-2020:5571)	Vulnerability - level 3	Vuln
239015	Red Hat Update for dnsmasq (RHSA-2021:0152)	Vulnerability - level 4	Vuln
239018	Red Hat Update for dnsmasq (RHSA-2021:0151)	Vulnerability - level 4	Vuln
239019	Red Hat Update for dnsmasq (RHSA-2021:0150)	Vulnerability - level 4	Vuln
239024	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2021:0056)	Vulnerability - level 4	Vuln
239062	Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 SP6 (RHSA-2021:0486)	Vulnerability - level 2	Vuln
239072	Red Hat Update for kernel (RHSA-2021:0558)	Vulnerability - level 4	Vuln
239076	Red Hat Update for nodejs:10 (RHSA-2021:0548)	Vulnerability - level 3	Vuln
239078	Red Hat Update for kernel-rt (RHSA-2021:0537)	Vulnerability - level 4	Vuln
239084	Red Hat Update for rh-nodejs10-nodejs (RHSA-2021:0521)	Vulnerability - level 3	Vuln
239111	Red Hat Update for grub2 (RHSA-2021:0701)	Vulnerability - level 3	Vuln
239112	Red Hat Update for grub2 (RHSA-2021:0700)	Vulnerability - level 3	Vuln
239113	Red Hat Update for grub2 (RHSA-2021:0699)	Vulnerability - level 3	Vuln
239114	Red Hat Update for grub2 (RHSA-2021:0698)	Vulnerability - level 3	Vuln
239115	Red Hat Update for grub2 (RHSA-2021:0697)	Vulnerability - level 3	Vuln
239116	Red Hat Update for grub2 (RHSA-2021:0696)	Vulnerability - level 3	Vuln
239117	Red Hat Update for bind (RHSA-2021:0691)	Vulnerability - level 4	Vuln
239119	Red Hat Update for kernel (RHSA-2021:0686)	Vulnerability - level 4	Vuln
239121	Red Hat Update for bind (RHSA-2021:0672)	Vulnerability - level 4	Vuln
239122	Red Hat Update for bind (RHSA-2021:0671)	Vulnerability - level 4	Vuln
239123	Red Hat Update for bind (RHSA-2021:0670)	Vulnerability - level 4	Vuln
239124	Red Hat Update for bind (RHSA-2021:0669)	Vulnerability - level 4	Vuln
239129	Red Hat Update for kernel (RHSA-2021:0765)	Vulnerability - level 4	Vuln
239131	Red Hat Update for nodejs:14 (RHSA-2021:0744)	Vulnerability - level 4	Vuln
239133	Red Hat Update for nodejs:10 (RHSA-2021:0741)	Vulnerability - level 4	Vuln
239134	Red Hat Update for nodejs:12 (RHSA-2021:0740)	Vulnerability - level 4	Vuln
239135	Red Hat Update for nodejs:12 (RHSA-2021:0739)	Vulnerability - level 4	Vuln
239136	Red Hat Update for nodejs:10 (RHSA-2021:0738)	Vulnerability - level 4	Vuln
239138	Red Hat Update for nodejs:10 (RHSA-2021:0735)	Vulnerability - level 4	Vuln
239139	Red Hat Update for nodejs:12 (RHSA-2021:0734)	Vulnerability - level 4	Vuln
239141	Red Hat Update for bind (RHSA-2021:0727)	Vulnerability - level 4	Vuln
239143	Red Hat Update for bind (RHSA-2021:0922)	Vulnerability - level 4	Vuln
239150	Red Hat Update for kernel-rt (RHSA-2021:0857)	Vulnerability - level 4	Vuln
239151	Red Hat Update for kernel (RHSA-2021:0856)	Vulnerability - level 4	Vuln
239152	Red Hat Update for rh-nodejs12-nodejs (RHSA-2021:0831)	Vulnerability - level 4	Vuln
239153	Red Hat Update for rh-nodejs14-nodejs (RHSA-2021:0830)	Vulnerability - level 4	Vuln
239154	Red Hat Update for rh-nodejs10-nodejs (RHSA-2021:0827)	Vulnerability - level 4	Vuln
239168	Red Hat Update for openvswitch2.11 and ovn2.11 (RHSA-2021:0931)	Vulnerability - level 4	Vuln
239185	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2021:1024)	Vulnerability - level 4	Vuln
239201	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2021:1131)	Vulnerability - level 4	Vuln
239247	Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 SP7 (RHSA-2021:1199)	Vulnerability - level 4	Vuln
239249	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2021:1063)	Vulnerability - level 4	Vuln

239251	Red Hat Update for openldap (RHSA-2021:1389)	Vulnerability - level 3	Vuln
239267	Red Hat Update for bind (RHSA-2021:1478)	Vulnerability - level 4	Vuln
239268	Red Hat Update for bind (RHSA-2021:1477)	Vulnerability - level 4	Vuln
239269	Red Hat Update for bind (RHSA-2021:1469)	Vulnerability - level 4	Vuln
239279	Red Hat Update for bind (RHSA-2021:2028)	Vulnerability - level 4	Vuln
239283	Red Hat Update for bind (RHSA-2021:2024)	Vulnerability - level 4	Vuln
239284	Red Hat Update for bind (RHSA-2021:1989)	Vulnerability - level 4	Vuln
239298	Red Hat Update for libvncserver (RHSA-2021:1811)	Vulnerability - level 3	Vuln
239315	Red Hat Update for shim (RHSA-2021:1734)	Vulnerability - level 3	Vuln
239328	Red Hat Update for curl (RHSA-2021:1610)	Vulnerability - level 3	Vuln
239344	Red Hat Update for kernel (RHSA-2021:1531)	Vulnerability - level 4	Vuln
239373	Red Hat Update for Red Hat OpenStack Platform 10.0 (openvswitch) (RHSA-2021:2205)	Vulnerability - level 4	Vuln
239382	Red Hat Update for postgresql:13 (RHSA-2021:2375)	Vulnerability - level 4	Vuln
239383	Red Hat Update for postgresql:12 (RHSA-2021:2372)	Vulnerability - level 4	Vuln
239389	Red Hat Update for postgresql:10 (RHSA-2021:2361)	Vulnerability - level 4	Vuln
239390	Red Hat Update for postgresql:9.6 (RHSA-2021:2360)	Vulnerability - level 4	Vuln
239405	Red Hat Update for microcode_ctl (RHSA-2021:2308)	Vulnerability - level 4	Vuln
239406	Red Hat Update for microcode_ctl (RHSA-2021:2307)	Vulnerability - level 4	Vuln
239407	Red Hat Update for microcode_ctl (RHSA-2021:2306)	Vulnerability - level 4	Vuln
239408	Red Hat Update for microcode_ctl (RHSA-2021:2305)	Vulnerability - level 4	Vuln
239409	Red Hat Update for microcode_ctl (RHSA-2021:2304)	Vulnerability - level 4	Vuln
239427	Red Hat Update for Red Hat OpenStack Platform 13.0 (RHSA-2021:2456)	Vulnerability - level 4	Vuln
239434	Red Hat Update for postgresql (RHSA-2021:2397)	Vulnerability - level 4	Vuln
239435	Red Hat Update for rh-postgresql13-postgresql (RHSA-2021:2396)	Vulnerability - level 4	Vuln
239436	Red Hat Update for rh-postgresql10-postgresql (RHSA-2021:2395)	Vulnerability - level 4	Vuln
239437	Red Hat Update for rh-postgresql12-postgresql (RHSA-2021:2394)	Vulnerability - level 4	Vuln
239438	Red Hat Update for postgresql:9.6 (RHSA-2021:2393)	Vulnerability - level 4	Vuln
239439	Red Hat Update for postgresql:10 (RHSA-2021:2392)	Vulnerability - level 4	Vuln
239440	Red Hat Update for postgresql:9.6 (RHSA-2021:2391)	Vulnerability - level 4	Vuln
239441	Red Hat Update for postgresql:10 (RHSA-2021:2390)	Vulnerability - level 4	Vuln
239442	Red Hat Update for postgresql:12 (RHSA-2021:2389)	Vulnerability - level 4	Vuln
239451	Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 SP8 (RHSA-2021:2472)	Vulnerability - level 4	Vuln
239456	Red Hat Update for kernel-rt (RHSA-2021:0774)	Vulnerability - level 4	Vuln
239468	Red Hat Update for libxml2 (RHSA-2021:2569)	Vulnerability - level 3	Vuln
239469	Red Hat Update for fwupd (RHSA-2021:2566)	Vulnerability - level 3	Vuln
239494	Red Hat Update for shim and fwupd (RHSA-2021:2790)	Vulnerability - level 3	Vuln
239533	Red Hat Update for microcode_ctl (RHSA-2021:3029)	Vulnerability - level 4	Vuln
239534	Red Hat Update for microcode_ctl (RHSA-2021:3028)	Vulnerability - level 4	Vuln
239535	Red Hat Update for microcode_ctl (RHSA-2021:3027)	Vulnerability - level 4	Vuln
239569	Red Hat Update for microcode_ctl (RHSA-2021:3176)	Vulnerability - level 4	Vuln
239590	Red Hat Update for rh-nodejs12-nodejs and rh-nodejs12-nodejs-nodemon (RHSA-2021:3281)	Vulnerability - level 4	Vuln
239591	Red Hat Update for rh-nodejs14-nodejs and rh-nodejs14-nodejs-nodemon (RHSA-2021:3280)	Vulnerability - level 4	Vuln
239598	Red Hat Update for microcode_ctl (RHSA-2021:3364)	Vulnerability - level 4	Vuln
239604	Red Hat Update for bind (RHSA-2021:3325)	Vulnerability - level 3	Vuln
239645	Red Hat Update for nodejs:12 (RHSA-2021:3623)	Vulnerability - level 4	Vuln
239654	Red Hat Update for nodejs:12 (RHSA-2021:3639)	Vulnerability - level 4	Vuln
239655	Red Hat Update for nodejs:12 (RHSA-2021:3638)	Vulnerability - level 4	Vuln
239657	Red Hat Update for shim and fwupd (RHSA-2021:3675)	Vulnerability - level 3	Vuln
239658	Red Hat Update for nodejs:14 (RHSA-2021:3666)	Vulnerability - level 4	Vuln
239671	Red Hat Update for httpd:2.4 (RHSA-2021:3816)	Vulnerability - level 4	Vuln
239678	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2021:3798)	Vulnerability - level 3	Vuln
239730	Red Hat Update for red hat jboss web server 5.4.2 (RHSA-2021:1195)	Vulnerability - level 4	Vuln

239735	Red Hat Update for red hat jboss web server 5.4.1 (RHSA-2021:0494)	Vulnerability - level 3	Vuln
239738	Red Hat Update for red hat jboss web server 3.1 service pack 11 (RHSA-2021:0489)	Vulnerability - level 2	Vuln
239739	Red Hat Update for red hat jboss web server 3.1 service pack 12 (RHSA-2021:1202)	Vulnerability - level 4	Vuln
239793	Red Hat Update for edk2 security (RHSA-2021:4198)	Vulnerability - level 3	Vuln
239801	Red Hat Update for bind (RHSA-2021:4384)	Vulnerability - level 3	Vuln
239803	Red Hat Update for go-toolset:rhel8 security (RHSA-2021:4156)	Vulnerability - level 3	Vuln
239816	Red Hat Update for kernel security (RHSA-2021:4356)	Vulnerability - level 3	Vuln
239823	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2021:4424)	Vulnerability - level 3	Vuln
239830	Red Hat Update for sqlite (RHSA-2021:4396)	Vulnerability - level 3	Vuln
239865	Red Hat Update for red hat jboss core services apache Hypertext Transfer Protocol (HTTP) server 2.4.37 sp10 (RHSA-2021:4614)	Vulnerability - level 3	Vuln
239871	Red Hat Update for httpd:2.4 (RHSA-2021:4537)	Vulnerability - level 4	Vuln
239879	Red Hat Update for kernel-rt (RHSA-2021:4140)	Vulnerability - level 3	Vuln
239884	Red Hat Update for kernel (RHSA-2021:4647)	Vulnerability - level 4	Vuln
239887	Red Hat Update for kernel-rt (RHSA-2021:4648)	Vulnerability - level 4	Vuln
239890	Red Hat Update for kernel security (RHSA-2021:4650)	Vulnerability - level 4	Vuln
239892	Red Hat Update for kernel-rt (RHSA-2021:4646)	Vulnerability - level 4	Vuln
239917	Red Hat Update for kernel (RHSA-2021:4871)	Vulnerability - level 4	Vuln
239918	Red Hat Update for kernel-rt (RHSA-2021:4875)	Vulnerability - level 4	Vuln
239964	Red Hat Update for go-toolset:rhel8 (RHSA-2021:5160)	Vulnerability - level 4	Vuln
239977	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2021:5226)	Vulnerability - level 3	Vuln
239981	Red Hat Update for grafana (RHSA-2022:0001)	Vulnerability - level 4	Vuln
239983	Red Hat Update for grafana (RHSA-2022:0002)	Vulnerability - level 4	Vuln
239986	Red Hat Update for rh-nodejs14-nodejs and rh-nodejs14-nodejs-nodemon (RHSA-2022:0041)	Vulnerability - level 3	Vuln
239990	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2022:0064)	Vulnerability - level 3	Vuln
240007	Red Hat Update for httpd (RHSA-2022:0143)	Vulnerability - level 4	Vuln
240023	Red Hat Update for OpenStack Platform 16.2 (RHSA-2022:0237)	Vulnerability - level 4	Vuln
240030	Red Hat Update for OpenStack Platform 16.1 (RHSA-2022:0260)	Vulnerability - level 4	Vuln
240037	Red Hat Update for nodejs:14 security (RHSA-2022:0246)	Vulnerability - level 5	Vuln
240051	Red Hat Update for nodejs:14 security (RHSA-2022:0350)	Vulnerability - level 5	Vuln
240099	Red Hat Update for openldap (RHSA-2022:0621)	Vulnerability - level 3	Vuln
240106	Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2022:0557)	Vulnerability - level 3	Vuln
240124	Red Hat Update for firefox (RHSA-2022:0817)	Vulnerability - level 5	Vuln
240132	Red Hat Update for firefox (RHSA-2022:0824)	Vulnerability - level 5	Vuln
240133	Red Hat Update for firefox (RHSA-2022:0818)	Vulnerability - level 5	Vuln
240136	Red Hat Update for firefox (RHSA-2022:0816)	Vulnerability - level 5	Vuln
240138	Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:0055)	Vulnerability - level 4	Vuln
240141	Red Hat Update for thunderbird (RHSA-2022:0853)	Vulnerability - level 5	Vuln
240142	Red Hat Update for thunderbird (RHSA-2022:0845)	Vulnerability - level 5	Vuln
240143	Red Hat Update for thunderbird (RHSA-2022:0843)	Vulnerability - level 5	Vuln
240145	Red Hat Update for thunderbird (RHSA-2022:0850)	Vulnerability - level 5	Vuln
240149	Red Hat Update for httpd:2.4 (RHSA-2022:0891)	Vulnerability - level 5	Vuln
240152	Red Hat Update for libxml2 (RHSA-2022:0899)	Vulnerability - level 4	Vuln
240155	Red Hat Update for expat (RHSA-2022:0951)	Vulnerability - level 4	Vuln
240161	Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:0927)	Vulnerability - level 4	Vuln
240166	Red Hat Update for expat (RHSA-2022:1012)	Vulnerability - level 5	Vuln
240168	Red Hat Update for httpd:2.4 (RHSA-2022:1049)	Vulnerability - level 5	Vuln
240169	Red Hat Update for httpd (RHSA-2022:1045)	Vulnerability - level 5	Vuln
240186	Red Hat Update for expat (RHSA-2022:1069)	Vulnerability - level 4	Vuln

240187	Red Hat Update for expat (RHSA-2022:1070)	Vulnerability - level 5	Vuln
240190	Red Hat Update for httpd:2.4 (RHSA-2022:1072)	Vulnerability - level 5	Vuln
240191	Red Hat Update for httpd24-httpd (RHSA-2022:1075)	Vulnerability - level 5	Vuln
240193	Red Hat Update for httpd:2.4 (RHSA-2022:1102)	Vulnerability - level 5	Vuln
240235	Red Hat Update for JBoss Core Services (RHSA-2022:1389)	Vulnerability - level 5	Vuln
240245	Red Hat Update for xmlrpc-c (RHSA-2022:1540)	Vulnerability - level 5	Vuln
240247	Red Hat Update for xmlrpc-c (RHSA-2022:1644)	Vulnerability - level 5	Vuln
240251	Red Hat Update for xmlrpc-c (RHSA-2022:1643)	Vulnerability - level 5	Vuln
240275	Red Hat Update for kernel-rt (RHSA-2022:1975)	Vulnerability - level 5	Vuln
240276	Red Hat Update for go-toolset:rhel8 (RHSA-2022:1819)	Vulnerability - level 5	Vuln
240291	Red Hat Update for bind security (RHSA-2022:2092)	Vulnerability - level 3	Vuln
240298	Red Hat Update for kernel security (RHSA-2022:1988)	Vulnerability - level 4	Vuln
240389	Red Hat Update for expat (RHSA-2022:4834)	Vulnerability - level 5	Vuln
240414	Red Hat Update for rh-nodejs12-nodejs security (RHSA-2022:4914)	Vulnerability - level 5	Vuln
240484	Red Hat Update for kernel-rt (RHSA-2022:5236)	Vulnerability - level 4	Vuln
240485	Red Hat Update for kernel (RHSA-2022:5232)	Vulnerability - level 4	Vuln
240494	Red Hat Update for kernel (RHSA-2022:5220)	Vulnerability - level 4	Vuln
240497	Red Hat Update for expat (RHSA-2022:5244)	Vulnerability - level 4	Vuln
240499	Red Hat Update for kernel (RHSA-2022:5249)	Vulnerability - level 4	Vuln
240503	Red Hat Update for go-toolset:rhel8 (RHSA-2022:5337)	Vulnerability - level 4	Vuln
240505	Red Hat Update for expat (RHSA-2022:5314)	Vulnerability - level 4	Vuln
240527	Red Hat Update for kernel-rt (RHSA-2022:5267)	Vulnerability - level 4	Vuln
240531	Red Hat Update for kernel-rt (RHSA-2022:5224)	Vulnerability - level 4	Vuln
240541	Red Hat Update for kernel security (RHSA-2022:5564)	Vulnerability - level 4	Vuln
240542	Red Hat Update for kernel-rt (RHSA-2022:5565)	Vulnerability - level 4	Vuln
240544	Red Hat Update for kernel-rt (RHSA-2022:5633)	Vulnerability - level 4	Vuln
240545	Red Hat Update for kernel (RHSA-2022:5626)	Vulnerability - level 4	Vuln
240578	Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:5729)	Vulnerability - level 4	Vuln
240588	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2022:5818)	Vulnerability - level 3	Vuln
240599	Red Hat Update for kernel-rt (RHSA-2022:5934)	Vulnerability - level 4	Vuln
240603	Red Hat Update for kernel (RHSA-2022:5998)	Vulnerability - level 4	Vuln
240607	Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2022:5068)	Vulnerability - level 5	Vuln
240616	Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:6094)	Vulnerability - level 5	Vuln
240641	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2022:6224)	Vulnerability - level 3	Vuln
240643	Red Hat Update for kernel-rt (RHSA-2022:6248)	Vulnerability - level 4	Vuln
240644	Red Hat Update for kernel (RHSA-2022:6243)	Vulnerability - level 4	Vuln
240655	Red Hat Update for rh-nodejs14-nodejs and rh-nodejs14-nodejs-nodemon (RHSA-2022:6389)	Vulnerability - level 5	Vuln
240656	Red Hat Update for nodejs:14 (RHSA-2022:6448)	Vulnerability - level 5	Vuln
240660	Red Hat Update for nodejs:16 (RHSA-2022:6449)	Vulnerability - level 5	Vuln
240676	Red Hat Update for nodejs and nodejs-nodemon (RHSA-2022:6595)	Vulnerability - level 5	Vuln
240698	Red Hat Update for httpd24-httpd (RHSA-2022:6753)	Vulnerability - level 5	Vuln
240736	Red Hat Update for nodejs:14 (RHSA-2022:6985)	Vulnerability - level 5	Vuln
240776	Red Hat Update for kernel-rt (RHSA-2022:7134)	Vulnerability - level 4	Vuln
240782	Red Hat Update for kernel security (RHSA-2022:7110)	Vulnerability - level 4	Vuln
240794	Red Hat Update for JBoss Core Services (RHSA-2022:7143)	Vulnerability - level 5	Vuln
240808	Red Hat Update for pcs (RHSA-2022:7343)	Vulnerability - level 3	Vuln
240815	Red Hat Update for kernel-rt (RHSA-2022:7444)	Vulnerability - level 4	Vuln
240817	Red Hat Update for kernel security (RHSA-2022:7683)	Vulnerability - level 4	Vuln
240822	Red Hat Update for bind (RHSA-2022:7790)	Vulnerability - level 4	Vuln
240828	Red Hat Update for bind9.16 (RHSA-2022:7643)	Vulnerability - level 4	Vuln

240829	Red Hat Update for container-tools:rhel8 security (RHSA-2022:7457)	Vulnerability - level 4	Vuln
240835	Red Hat Update for xmlrpc-c (RHSA-2022:7692)	Vulnerability - level 3	Vuln
240840	Red Hat Update for e2fsprogs (RHSA-2022:7720)	Vulnerability - level 4	Vuln
240854	Red Hat Update for httpd:2.4 (RHSA-2022:7647)	Vulnerability - level 3	Vuln
240869	Red Hat Update for kernel-rt (RHSA-2022:7933)	Vulnerability - level 4	Vuln
240885	Red Hat Update for httpd security (RHSA-2022:8067)	Vulnerability - level 5	Vuln
240888	Red Hat Update for bind (RHSA-2022:8068)	Vulnerability - level 4	Vuln
240901	Red Hat Update for dhcp (RHSA-2022:8385)	Vulnerability - level 4	Vuln
240904	Red Hat Update for kernel security (RHSA-2022:8267)	Vulnerability - level 4	Vuln
240917	Red Hat Update for e2fsprogs (RHSA-2022:8361)	Vulnerability - level 4	Vuln
240996	Red Hat Update for JBoss Core Services (RHSA-2022:8840)	Vulnerability - level 5	Vuln
241122	Red Hat Update for bind (RHSA-2023:0402)	Vulnerability - level 4	Vuln
241125	Red Hat Update for kernel (RHSA-2023:0399)	Vulnerability - level 4	Vuln
241126	Red Hat Update for kernel-rt (RHSA-2023:0400)	Vulnerability - level 4	Vuln
241153	Red Hat Update for JBoss Enterprise Application Platform 7.4.9 (RHSA-2023:0554)	Vulnerability - level 5	Vuln
241154	Red Hat Update for JBoss Enterprise Application Platform 7.4.9 (RHSA-2023:0552)	Vulnerability - level 5	Vuln
241155	Red Hat Update for JBoss Enterprise Application Platform 7.4.9 (RHSA-2023:0553)	Vulnerability - level 5	Vuln
241227	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:0946)	Vulnerability - level 4	Vuln
241256	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1199)	Vulnerability - level 4	Vuln
241274	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1335)	Vulnerability - level 4	Vuln
241285	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1405)	Vulnerability - level 4	Vuln
241291	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1440)	Vulnerability - level 4	Vuln
241292	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1441)	Vulnerability - level 4	Vuln
241396	Red Hat Update for edk2 (RHSA-2023:2022)	Vulnerability - level 4	Vuln
241469	Red Hat Update for edk2 security (RHSA-2023:2165)	Vulnerability - level 4	Vuln
241496	Red Hat Update for edk2 (RHSA-2023:2932)	Vulnerability - level 4	Vuln
241568	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:3408)	Vulnerability - level 3	Vuln
241574	Red Hat Update for JBoss Core Services (RHSA-2023:3354)	Vulnerability - level 4	Vuln
241614	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1437)	Vulnerability - level 4	Vuln
241652	Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1439)	Vulnerability - level 4	Vuln
256010	CentOS Security Update for openssl (CESA-2016:0722)	Vulnerability - level 4	Vuln
256021	CentOS Security Update for ntp Security Update (CESA-2016:0780)	Vulnerability - level 3	Vuln
256022	CentOS Security Update for openssh (CESA-2016:0741)	Vulnerability - level 3	Vuln
256023	CentOS Security Update for openssl (CESA-2016:0996)	Vulnerability - level 4	Vuln
256026	CentOS Security Update for squid34 (CESA-2016:1140)	Vulnerability - level 3	Vuln
256027	CentOS Security Update for ntp (CESA-2016:1141)	Vulnerability - level 3	Vuln
256028	CentOS Security Update for squid (CESA-2016:1139)	Vulnerability - level 3	Vuln
256029	CentOS Security Update for openssl (CESA-2016:1137)	Vulnerability - level 4	Vuln
256041	CentOS Security Update for httpd (CESA-2016:1421) (HTTPoxy)	Vulnerability - level 4	Vuln
256042	CentOS Security Update for httpd (CESA-2016:1422) (HTTPoxy)	Vulnerability - level 4	Vuln
256054	CentOS Security Update for php (CESA-2016:1609)	Vulnerability - level 3	Vuln
256056	CentOS Security Update for php (CESA-2016:1613)	Vulnerability - level 3	Vuln
256069	CentOS Security Update for tomcat6 (CESA-2016:2045)	Vulnerability - level 4	Vuln
256071	CentOS Security Update for tomcat (CESA-2016:2046)	Vulnerability - level 4	Vuln
256101	CentOS Security Update for tomcat (CESA-2016:2599)	Vulnerability - level 3	Vuln
256105	CentOS Security Update for curl (CESA-2016:2575)	Vulnerability - level 3	Vuln

256110	CentOS Security Update for openssl (CESA-2016:1940)	Vulnerability - level 4	Vuln
256128	CentOS Security Update for ntp (CESA-2016:2583)	Vulnerability - level 3	Vuln
256129	CentOS Security Update for openssh (CESA-2016:2588)	Vulnerability - level 3	Vuln
256161	CentOS Security Update for ntp (CESA-2017:0252)	Vulnerability - level 3	Vuln
256195	CentOS Security Update for openssh (CESA-2017:0641)	Vulnerability - level 3	Vuln
256248	CentOS Security Update for java-1.8.0-openjdk (CESA-2017:1789)	Vulnerability - level 5	Vuln
256251	CentOS Security Update for java-1.7.0-openjdk (CESA-2017:2424)	Vulnerability - level 4	Vuln
256257	CentOS Security Update for curl Security Update (CESA-2017:2016)	Vulnerability - level 4	Vuln
256273	CentOS Security Update for openssh (CESA-2017:2029)	Vulnerability - level 4	Vuln
256274	CentOS Security Update for pidgin (CESA-2017:1854)	Vulnerability - level 4	Vuln
256295	CentOS Security Update for mercurial (CESA-2017:2489)	Vulnerability - level 4	Vuln
256319	CentOS Security Update for wpa_supplicant (CESA-2017:2907) (KRACK Attack)	Vulnerability - level 4	Vuln
256320	CentOS Security Update for wpa_supplicant (CESA-2017:2911) (KRACK Attack)	Vulnerability - level 4	Vuln
256323	CentOS Security Update for kernel (CESA-2017:2930)	Vulnerability - level 4	Vuln
256343	CentOS Security Update for java-1.7.0-openjdk (CESA-2017:3392)	Vulnerability - level 4	Vuln
256374	CentOS Security Update for quagga (CESA-2018:0377)	Vulnerability - level 4	Vuln
256394	CentOS Security Update for openssh (CESA-2018:0980)	Vulnerability - level 4	Vuln
256395	CentOS Security Update for Open Secure Sockets Layer (OpenSSL) (CESA-2018:0998)	Vulnerability - level 4	Vuln
256474	CentOS Security Update for kernel Security Update (CESA-2018:2390)	Vulnerability - level 4	Vuln
256475	CentOS Security Update for kernel Security Update (CESA-2018:2384)	Vulnerability - level 4	Vuln
256524	CentOS Security Update for Open Secure Sockets Layer (OpenSSL) (CESA-2018:3221)	Vulnerability - level 4	Vuln
256530	CentOS Security Update for wpa_supplicant (CESA-2018:3107)	Vulnerability - level 4	Vuln
256531	CentOS Security Update for xerces-c (CESA-2018:3335)	Vulnerability - level 4	Vuln
256597	CentOS Security Update for python (CESA-2019:0710)	Vulnerability - level 4	Vuln
256623	CentOS Security Update for python (CESA-2019:1467)	Vulnerability - level 4	Vuln
256626	CentOS Security Update for python (CESA-2019:1587)	Vulnerability - level 4	Vuln
256647	CentOS Security Update for curl (CESA-2019:1880)	Vulnerability - level 4	Vuln
256658	CentOS Security Update for curl (CESA-2019:2181)	Vulnerability - level 4	Vuln
256688	CentOS Security Update for nss-util (CESA-2019:2237)	Vulnerability - level 4	Vuln
256709	CentOS Security Update for tomcat (CESA-2019:2205)	Vulnerability - level 4	Vuln
256742	CentOS Security Update for nss-softoken (CESA-2019:4152)	Vulnerability - level 4	Vuln
256751	CentOS Security Update for nss (CESA-2019:4190)	Vulnerability - level 4	Vuln
256801	CentOS Security Update for libvncserver (CESA-2020:0913)	Vulnerability - level 4	Vuln
256909	CentOS Security Update for microcode_ctl (CESA-2020:2433)	Vulnerability - level 4	Vuln
256910	CentOS Security Update for kernel Security Update (CESA-2020:2430)	Vulnerability - level 4	Vuln
256911	CentOS Security Update for microcode_ctl (CESA-2020:2432)	Vulnerability - level 4	Vuln
256916	CentOS Security Update for kernel Security Update (CESA-2020:2664)	Vulnerability - level 4	Vuln
256935	CentOS Security Update for grub2 (CESA-2020:3217)	Vulnerability - level 4	Vuln
256939	CentOS Security Update for libvncserver (CESA-2020:3281)	Vulnerability - level 4	Vuln
256964	CentOS Security Update for ipa Security Update (CESA-2020:3936)	Vulnerability - level 3	Vuln
256998	CentOS Security Update for libxml2 (CESA-2020:3996)	Vulnerability - level 4	Vuln
257006	CentOS Security Update for subversion (CESA-2020:3972)	Vulnerability - level 2	Vuln
257036	CentOS Security Update for microcode_ctl (CESA-2020:5083)	Vulnerability - level 4	Vuln
257049	CentOS Security Update for Open Secure Sockets Layer (OpenSSL) (CESA-2020:5566)	Vulnerability - level 2	Vuln
257067	CentOS Security Update for bind (CESA-2021:0671)	Vulnerability - level 4	Vuln
257070	CentOS Security Update for kernel (CESA-2021:0856)	Vulnerability - level 4	Vuln
257082	CentOS Security Update for bind (CESA-2021:1469)	Vulnerability - level 4	Vuln
257102	CentOS Security Update for microcode_ctl (CESA-2021:3028)	Vulnerability - level 4	Vuln
257112	CentOS Security Update for bind (CESA-2021:3325)	Vulnerability - level 3	Vuln

257128	CentOS Security Update for Open Secure Sockets Layer (OpenSSL) (CESA-2021:3798)	Vulnerability - level 3	Vuln
257148	CentOS Security Update for httpd (CESA-2022:0143)	Vulnerability - level 5	Vuln
257157	CentOS Security Update for openldap (CESA-2022:0621)	Vulnerability - level 4	Vuln
257160	CentOS Security Update for expat (CESA-2022:1069)	Vulnerability - level 5	Vuln
257161	CentOS Security Update for firefox (CESA-2022:0824)	Vulnerability - level 5	Vuln
257162	CentOS Security Update for httpd (CESA-2022:1045)	Vulnerability - level 5	Vuln
257164	CentOS Security Update for thunderbird (CESA-2022:0850)	Vulnerability - level 5	Vuln
257172	CentOS Security Update for kernel (CESA-2022:5232)	Vulnerability - level 4	Vuln
257210	CentOS Security Update for kernel (CESA-2023:0399)	Vulnerability - level 4	Vuln
257214	CentOS Security Update for bind (CESA-2023:0402)	Vulnerability - level 4	Vuln
257231	CentOS Security Update for Open Secure Sockets Layer (OpenSSL) (CESA-2023:1335)	Vulnerability - level 4	Vuln
27377	Core FTP Server Local Code Execution Vulnerability	Potential Vulnerability - level 3	Practice
27377	Mooseguy Blog System 'blog.php' SQL Injection Vulnerability	Potential Vulnerability - level 3	
276056	Fedora Security Update for openssh (FEDORA-2016-7f5004093e)	Vulnerability - level 3	Vuln
276082	Fedora Security Update for openssl (FEDORA-2016-1411324654)	Vulnerability - level 3	Vuln
276090	Fedora Security Update for ntp (FEDORA-2016-5b2eb0bf9c)	Vulnerability - level 3	Vuln
276113	Fedora Security Update for openssl (FEDORA-2016-1e39d934ed)	Vulnerability - level 3	Vuln
276139	Fedora Security Update for curl (FEDORA-2016-7a2ed52d41)	Vulnerability - level 3	Vuln
276143	Fedora Security Update for curl (FEDORA-2016-08533fc59c)	Vulnerability - level 3	Vuln
276154	Fedora Security Update for openvpn (FEDORA-2016-7810e24465)	Vulnerability - level 3	Vuln
276167	Fedora Security Update for openssl (FEDORA-2016-a555159613)	Vulnerability - level 3	Vuln
276189	Fedora Security Update for curl (FEDORA-2016-80f4f71eff)	Vulnerability - level 3	Vuln
276255	Fedora Security Update for curl (FEDORA-2016-89769648a0)	Vulnerability - level 3	Vuln
276256	Fedora Security Update for curl (FEDORA-2016-e8e8cdb4ed)	Vulnerability - level 3	Vuln
276275	Fedora Security Update for tomcat (FEDORA-2016-4094bd4ad6)	Vulnerability - level 3	Vuln
276308	Fedora Security Update for openssl (FEDORA-2016-e6807b3394) and (FEDORA-2016-2802690366)	Vulnerability - level 3	Vuln
276309	Fedora Security Update for openssl (FEDORA-2016-64e0743e16), (FEDORA-2016-97454404fe) and (FEDORA-2016-a555159613)	Vulnerability - level 3	Vuln
276310	Fedora Security Update for curl (FEDORA-2016-edbb33ab2e)	Vulnerability - level 3	Vuln
276346	Fedora Security Update for ntp5 (FEDORA-2016-c198d15316)	Vulnerability - level 3	Vuln
276355	Fedora Security Update for curl (FEDORA-2016-86d2b5aefb)	Vulnerability - level 3	Vuln
276368	Fedora Security Update for opensshp1 (FEDORA-2017-4767e2991d)	Vulnerability - level 3	Vuln
276549	Fedora Security Update for ntp5 (FEDORA-2017-5ebac1c112)	Vulnerability - level 3	Vuln
276557	Fedora Security Update for kernel (FEDORA-2017-02174df32f)	Vulnerability - level 3	Vuln
276558	Fedora Security Update for kernel (FEDORA-2017-93dec9eba5)	Vulnerability - level 3	Vuln
276690	Fedora Security Update for ansible (FEDORA-2017-6aff7475b7)	Vulnerability - level 3	Vuln
276706	Fedora Security Update for Linux Kernel (FEDORA-2013-12339)	Vulnerability - level 4	Vuln
276759	Fedora Security Update for java-1.8.0-openjdk (FEDORA-2017-605557de96)	Vulnerability - level 3	Vuln
276928	Fedora Security Update for wpa_supplicant (FEDORA-2017-12e76e8364) (KRACK Attack)	Vulnerability - level 3	Vuln
276929	Fedora Security Update for wpa_supplicant (FEDORA-2017-60bfb576b7) (KRACK Attack)	Vulnerability - level 3	Vuln
277014	Fedora Security Update for opensshp1 (FEDORA-2017-4862a3bfb1)	Vulnerability - level 3	Vuln
277015	Fedora Security Update for opensshp1 (FEDORA-2017-78f0991378)	Vulnerability - level 3	Vuln
277034	Fedora Security Update for opensslg (FEDORA-2017-dbec196dd8)	Vulnerability - level 3	Vuln
277035	Fedora Security Update for opensslm (FEDORA-2017-55a3247cfd)	Vulnerability - level 3	Vuln
277036	Fedora Security Update for compat-openssl10m (FEDORA-2017-7f30914972)	Vulnerability - level 3	Vuln
277056	Fedora Security Update for hostapd (FEDORA-2017-cfb950d8f4)	Vulnerability - level 3	Vuln
277114	Fedora Security Update for libxml2 (FEDORA-2018-db610fff5b)	Vulnerability - level 5	Vuln

277198	Fedora Security Update for quagga (FEDORA-2018-b3e985489b)	Vulnerability - level 3	Vuln
277415	Fedora Security Update for wpa_supplicant (FEDORA-2018-41dfadd21a)	Vulnerability - level 3	Vuln
277526	Fedora Security Update for curl (FEDORA-2018-fdc4ca8675)	Vulnerability - level 3	Vuln
277580	Fedora Security Update for Open Secure Sockets Layer (OpenSSL-1.1.0i) (FEDORA-2018-520e4c5b4e)	Vulnerability - level 3	Vuln
277614	Fedora Security Update for nss (FEDORA-2019-68b9bec5ca)	Vulnerability - level 3	Vuln
277706	Fedora Security Update for gpsd (FEDORA-2019-9a6906a128)	Vulnerability - level 3	Vuln
277760	Fedora Security Update for python3 (FEDORA-2019-243442e600)	Vulnerability - level 3	Vuln
277761	Fedora Security Update for python3 (FEDORA-2019-86f32cbab1)	Vulnerability - level 3	Vuln
277777	Fedora Security Update for python35 (FEDORA-2019-cf725dd20b)	Vulnerability - level 3	Vuln
277778	Fedora Security Update for python34 (FEDORA-2019-6baeb15da3)	Vulnerability - level 3	Vuln
277829	Fedora Security Update for drupal8 (FEDORA-2019-1a3edd7e8a)	Vulnerability - level 3	Vuln
277831	Fedora Security Update for drupal7 (FEDORA-2019-a06dffab1c)	Vulnerability - level 3	Vuln
277922	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2019-d15aac6c4e)	Vulnerability - level 3	Vuln
278063	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2019-d51641f152)	Vulnerability - level 3	Vuln
278064	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2019-9ab7ee6309)	Vulnerability - level 3	Vuln
278099	Fedora Security Update for python34 (FEDORA-2019-50772cf122)	Vulnerability - level 3	Vuln
278100	Fedora Security Update for python34 (FEDORA-2019-2b1f72899a)	Vulnerability - level 3	Vuln
278101	Fedora Security Update for python34 (FEDORA-2019-5dc275c9f2)	Vulnerability - level 3	Vuln
278102	Fedora Security Update for Compat-Open Secure Sockets Layer (compat-OpenSSL10) (FEDORA-2019-db06efdea1)	Vulnerability - level 3	Vuln
278103	Fedora Security Update for Compat-Open Secure Sockets Layer (compat-OpenSSL10) (FEDORA-2019-00c25b9379)	Vulnerability - level 3	Vuln
278104	Fedora Security Update for Compat-Open Secure Sockets Layer (compat-OpenSSL10) (FEDORA-2019-9a0a7c0986)	Vulnerability - level 3	Vuln
278360	Fedora Security Update for rssh (FEDORA-2019-d1487c13ac)	Vulnerability - level 4	Vuln
278361	Fedora Security Update for rssh (FEDORA-2019-e47add6b2b)	Vulnerability - level 4	Vuln
278363	Fedora Security Update for rssh (FEDORA-2019-bfb407659e)	Vulnerability - level 4	Vuln
278364	Fedora Security Update for Python (FEDORA-2019-d202cda4f8)	Vulnerability - level 3	Vuln
278366	Fedora Security Update for Python (FEDORA-2019-57462fa10d)	Vulnerability - level 3	Vuln
278368	Fedora Security Update for Python (FEDORA-2019-b06ec6159b)	Vulnerability - level 3	Vuln
278465	Fedora Security Update for python3 and python3-docs (FEDORA-2019-60a1defcd1)	Vulnerability - level 3	Vuln
278466	Fedora Security Update for python3 and python3-docs (FEDORA-2019-9bfb4a3e4b)	Vulnerability - level 3	Vuln
278482	Fedora Security Update for python36 (FEDORA-2019-7723d4774a)	Vulnerability - level 3	Vuln
278625	Fedora Security Update for python3 (FEDORA-2019-a122fe704d)	Vulnerability - level 3	Vuln
278629	Fedora Security Update for python34 (FEDORA-2019-6b02154aa0)	Vulnerability - level 3	Vuln
278630	Fedora Security Update for python35 (FEDORA-2019-6e1938a3c5)	Vulnerability - level 3	Vuln
278631	Fedora Security Update for python35 (FEDORA-2019-51f1e08207)	Vulnerability - level 3	Vuln
278632	Fedora Security Update for python34 (FEDORA-2019-7d9f3cf3ce)	Vulnerability - level 3	Vuln
278787	Fedora Security Update for nss (FEDORA-2018-a78b2ef820)	Vulnerability - level 3	Vuln
278814	Fedora Security Update for curl (FEDORA-2018-69bac0f51c)	Vulnerability - level 3	Vuln
278836	Fedora Security Update for curl (FEDORA-2018-7785911c9e)	Vulnerability - level 3	Vuln
278872	Fedora Security Update for xerces-c27 (FEDORA-2018-51ce232320)	Vulnerability - level 3	Vuln
278977	Fedora Security Update for curl (FEDORA-2018-7f83032de6)	Vulnerability - level 3	Vuln
278997	Fedora Security Update for proftpd (FEDORA-2020-876b1f664e)	Vulnerability - level 3	Vuln
278998	Fedora Security Update for proftpd (FEDORA-2020-76c707cff0)	Vulnerability - level 3	Vuln
279035	Fedora Security Update for libxml2 (FEDORA-2020-41fe1680f6)	Vulnerability - level 3	Vuln
279170	Fedora Security Update for rssh (FEDORA-2019-d1487c13ac)	Vulnerability - level 3	Vuln
279171	Fedora Security Update for rssh (FEDORA-2019-e47add6b2b)	Vulnerability - level 3	Vuln
279172	Fedora Security Update for rssh (FEDORA-2019-bfb407659e)	Vulnerability - level 3	Vuln
279173	Fedora Security Update for Python (FEDORA-2019-d202cda4f8)	Vulnerability - level 3	Vuln
279174	Fedora Security Update for Python (FEDORA-2019-57462fa10d)	Vulnerability - level 3	Vuln

279175	Fedora Security Update for Python (FEDORA-2019-b06ec6159b)	Vulnerability - level 3	Vuln
279535	Fedora Security Update for python3 (FEDORA-2019-ec26883852)	Vulnerability - level 3	Vuln
279536	Fedora Security Update for python3 (FEDORA-2019-1ffd6b6064)	Vulnerability - level 3	Vuln
279634	Fedora Security Update for subversion (FEDORA-2019-f6bc68e455)	Vulnerability - level 3	Vuln
279678	Fedora Security Update for drupal7 (FEDORA-2019-2a0ce0c58c)	Vulnerability - level 3	Vuln
279680	Fedora Security Update for drupal8 (FEDORA-2019-eba8e44ee6)	Vulnerability - level 3	Vuln
279681	Fedora Security Update for drupal8 (FEDORA-2019-7eaf0bbe7c)	Vulnerability - level 3	Vuln
279745	Fedora Security Update for python36 (FEDORA-2019-7df59302e0)	Vulnerability - level 3	Vuln
279801	Fedora Security Update for libxml2 (FEDORA-2020-0c71c00af4)	Vulnerability - level 3	Vuln
279909	Fedora Security Update for mingw-libxml2 (FEDORA-2020-7694e8be73)	Vulnerability - level 3	Vuln
279999	Fedora Security Update for sqlite (FEDORA-2020-0477f8840e)	Vulnerability - level 3	Vuln
280041	Fedora Security Update for kernel and kernel-headers (FEDORA-2020-e47d28bc2b)	Vulnerability - level 3	Vuln
280067	Fedora Security Update for kernel and kernel-headers (FEDORA-2020-3364913ace)	Vulnerability - level 3	Vuln
280079	Fedora Security Update for nghttp2-1.41.0-1.fc31 (FEDORA-2020-f7d15c8b77)	Vulnerability - level 3	Vuln
280085	Fedora Security Update for microcode_ctl (FEDORA-2020-e8835a5f8e)	Vulnerability - level 3	Vuln
280127	Fedora Security Update for microcode_ctl (FEDORA-2020-11ddbfbdf0)	Vulnerability - level 3	Vuln
280167	Fedora Security Update for libvncserver (FEDORA-2020-37112ac660)	Vulnerability - level 3	Vuln
280186	Fedora Security Update for libvncserver (FEDORA-2020-1a4b1c8271)	Vulnerability - level 3	Vuln
280519	Fedora Security Update for nodejs (FEDORA-2020-74bf23e1f1)	Vulnerability - level 3	Vuln
280562	Fedora Security Update for kernel, kernel-headers (FEDORA-2020-e211716d08)	Vulnerability - level 1	Vuln
280578	Fedora Security Update for Microcode (FEDORA-2020-14fda1bf85)	Vulnerability - level 1	Vuln
280598	Fedora Security Update for microcode_ctl (FEDORA-2020-1afbe7ba2d)	Vulnerability - level 1	Vuln
280621	Fedora Security Update for curl (FEDORA-2020-7ab62c73bc)	Vulnerability - level 3	Vuln
280627	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2020-a31b01e945)	Vulnerability - level 2	Vuln
280674	Fedora Security Update for curl (FEDORA-2020-ceaf490686)	Vulnerability - level 3	Vuln
280681	Fedora Security Update for nodejs (FEDORA-2020-43d5a372fc)	Vulnerability - level 3	Vuln
280728	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2020-ef1870065a)	Vulnerability - level 2	Vuln
280739	Fedora Security Update for microcode_ctl (FEDORA-2020-2c8824c6b1)	Vulnerability - level 1	Vuln
280741	Fedora Security Update for kernel, kernel-headers (FEDORA-2020-98ccae320c)	Vulnerability - level 1	Vuln
280834	Fedora Security Update for dnsmasq (FEDORA-2021-84440e87ba)	Vulnerability - level 3	Vuln
280997	Fedora Security Update for dnsmasq (FEDORA-2021-2e4c3d5a9d)	Vulnerability - level 4	Vuln
281155	Fedora Security Update for libxml2 (FEDORA-2021-e8b7e177a4)	Vulnerability - level 3	Vuln
281180	Fedora Security Update for libxml2 (FEDORA-2021-e3ed1ba38b)	Vulnerability - level 3	Vuln
281228	Fedora Security Update for bind (FEDORA-2021-47f23870ec)	Vulnerability - level 4	Vuln
281229	Fedora Security Update for bind (FEDORA-2021-ace61cbee1)	Vulnerability - level 4	Vuln
281363	Fedora Security Update for efi (FEDORA-2021-cab258a413)	Vulnerability - level 3	Vuln
281398	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2021-cbf14ab8f9)	Vulnerability - level 4	Vuln
281552	Fedora Security Update for nodejs (FEDORA-2021-a760169c3c)	Vulnerability - level 5	Vuln
281553	Fedora Security Update for nodejs (FEDORA-2021-f6bd75e9d4)	Vulnerability - level 5	Vuln
281554	Fedora Security Update for nodejs (FEDORA-2021-6aaba80ba2)	Vulnerability - level 5	Vuln
281555	Fedora Security Update for arm (FEDORA-2021-267c08cc40)	Vulnerability - level 3	Vuln
281556	Fedora Security Update for arm (FEDORA-2021-0fa2f42d3c)	Vulnerability - level 3	Vuln
281557	Fedora Security Update for arm (FEDORA-2021-332fb9c796)	Vulnerability - level 3	Vuln

281600	Fedora Security Update for bind (FEDORA-2021-8b4744f152)	Vulnerability - level 4	Vuln
281603	Fedora Security Update for dpdk (FEDORA-2021-fba11d37ee)	Vulnerability - level 3	Vuln
281607	Fedora Security Update for bind (FEDORA-2021-0595625865)	Vulnerability - level 4	Vuln
281608	Fedora Security Update for bind (FEDORA-2021-28f97e232d)	Vulnerability - level 4	Vuln
281707	Fedora Security Update for libxml2 (FEDORA-2021-b950000d2b)	Vulnerability - level 3	Vuln
281906	Fedora Security Update for golang (FEDORA-2021-38b51d9fd3)	Vulnerability - level 3	Vuln
281910	Fedora Security Update for Hypertext Transfer Protocol Daemon (HTTPd) (FEDORA-2021-dce7e7738e)	Vulnerability - level 3	Vuln
281921	Fedora Security Update for golang (FEDORA-2021-6a3024b3fd)	Vulnerability - level 3	Vuln
281996	Fedora Security Update for containerd (FEDORA-2021-df975338d4)	Vulnerability - level 3	Vuln
282051	Fedora Security Update for bind (FEDORA-2021-eb8dab50ba)	Vulnerability - level 3	Vuln
282052	Fedora Security Update for bind (FEDORA-2021-39b33260b8)	Vulnerability - level 3	Vuln
282073	Fedora Security Update for busybox (FEDORA-2021-c52c0fe490)	Vulnerability - level 3	Vuln
282074	Fedora Security Update for busybox (FEDORA-2021-5a95823596)	Vulnerability - level 3	Vuln
282113	Fedora Security Update for golang (FEDORA-2021-2ef35beebf)	Vulnerability - level 3	Vuln
282114	Fedora Security Update for golang (FEDORA-2021-2b2dd1b5a7)	Vulnerability - level 3	Vuln
282205	Fedora Security Update for golang (FEDORA-2021-29943703de)	Vulnerability - level 3	Vuln
282206	Fedora Security Update for golang (FEDORA-2021-6fdc5ea304)	Vulnerability - level 3	Vuln
282291	Fedora Security Update for grafana (FEDORA-2022-c6ae206be7)	Vulnerability - level 4	Vuln
282292	Fedora Security Update for grafana (FEDORA-2022-6e6b59a682)	Vulnerability - level 4	Vuln
282302	Fedora Security Update for qt5 (FEDORA-2022-ecdf338eb1)	Vulnerability - level 5	Vuln
282329	Fedora Security Update for qt5 (FEDORA-2022-e39987b17d)	Vulnerability - level 5	Vuln
282365	Fedora Security Update for mingw (FEDORA-2022-d2abd0858e)	Vulnerability - level 5	Vuln
282366	Fedora Security Update for mingw (FEDORA-2022-88f6a3d290)	Vulnerability - level 5	Vuln
282425	Fedora Security Update for libxml2 (FEDORA-2022-b661dea83d)	Vulnerability - level 3	Vuln
282449	Fedora Security Update for mingw (FEDORA-2022-3d9d67f558)	Vulnerability - level 5	Vuln
282450	Fedora Security Update for mingw (FEDORA-2022-04f206996b)	Vulnerability - level 5	Vuln
282462	Fedora Security Update for libxml2 (FEDORA-2022-050c712ed7)	Vulnerability - level 4	Vuln
282483	Fedora Security Update for Open Virtual Private Network (OpenVPN) (FEDORA-2022-a9bd17092d)	Vulnerability - level 4	Vuln
282491	Fedora Security Update for kernel (FEDORA-2022-9342e59a98)	Vulnerability - level 4	Vuln
282492	Fedora Security Update for kernel (FEDORA-2022-de4474b89d)	Vulnerability - level 4	Vuln
282499	Fedora Security Update for bind (FEDORA-2022-427cfc50f8)	Vulnerability - level 4	Vuln
282500	Fedora Security Update for httpd (FEDORA-2022-b4103753e9)	Vulnerability - level 5	Vuln
282519	Fedora Security Update for Open Virtual Private Network (OpenVPN) (FEDORA-2022-7d46acce7c)	Vulnerability - level 4	Vuln
282521	Fedora Security Update for httpd (FEDORA-2022-21264ec6db)	Vulnerability - level 5	Vuln
282526	Fedora Security Update for bind (FEDORA-2022-042d9c6146)	Vulnerability - level 3	Vuln
282579	Fedora Security Update for kernel (FEDORA-2022-91633399ff)	Vulnerability - level 4	Vuln
282580	Fedora Security Update for kernel (FEDORA-2022-5cd9d787dc)	Vulnerability - level 4	Vuln
282592	Fedora Security Update for dhcp (FEDORA-2022-a88218de5c)	Vulnerability - level 4	Vuln
282634	Fedora Security Update for dhcp (FEDORA-2022-05918f0838)	Vulnerability - level 4	Vuln
282771	Fedora Security Update for kernel (FEDORA-2022-8095b23575)	Vulnerability - level 4	Vuln
282772	Fedora Security Update for kernel (FEDORA-2022-014c3a24d9)	Vulnerability - level 4	Vuln
282773	Fedora Security Update for kernel (FEDORA-2022-b2cde267d9)	Vulnerability - level 4	Vuln
282790	Fedora Security Update for clash (FEDORA-2022-a49babad75)	Vulnerability - level 4	Vuln
282801	Fedora Security Update for gron (FEDORA-2022-53f0c619c5)	Vulnerability - level 4	Vuln
282860	Fedora Security Update for openssl1.1 (FEDORA-2022-b651cb69e6)	Vulnerability - level 5	Vuln
282873	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2022-c9c02865f6)	Vulnerability - level 5	Vuln
282878	Fedora Security Update for golang (FEDORA-2022-c0f780ecf1)	Vulnerability - level 4	Vuln
282882	Fedora Security Update for httpd (FEDORA-2022-e620fb15d5)	Vulnerability - level 5	Vuln
282887	Fedora Security Update for golang (FEDORA-2022-e46e6e8317)	Vulnerability - level 4	Vuln
282893	Fedora Security Update for 3mux (FEDORA-2022-fae3ecee19)	Vulnerability - level 5	Vuln
282896	Fedora Security Update for openssl1.1 (FEDORA-2022-3b7d0abd0b)	Vulnerability - level 5	Vuln
282903	Fedora Security Update for httpd (FEDORA-2022-b54a8dee29)	Vulnerability - level 5	Vuln

282924	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2022-3fdc2d3047)	Vulnerability - level 4	Vuln
282931	Fedora Security Update for apptainer (FEDORA-2022-ba365d3703)	Vulnerability - level 5	Vuln
282939	Fedora Security Update for openssl1.1 (FEDORA-2022-89a17be281)	Vulnerability - level 4	Vuln
282947	Fedora Security Update for 3mux (FEDORA-2022-3969b64d4b)	Vulnerability - level 5	Vuln
282968	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2022-41890e9e44)	Vulnerability - level 5	Vuln
283049	Fedora Security Update for fzf (FEDORA-2022-30c5ed5625)	Vulnerability - level 5	Vuln
283356	Fedora Security Update for nodejs (FEDORA-2022-de515f765f)	Vulnerability - level 4	Vuln
283357	Fedora Security Update for nodejs (FEDORA-2022-52dec6351a)	Vulnerability - level 4	Vuln
283432	Fedora Security Update for nodejs (FEDORA-2022-1667f7b60a)	Vulnerability - level 4	Vuln
283694	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2023-57f33242bc)	Vulnerability - level 4	Vuln
283709	Fedora Security Update for edk2 (FEDORA-2023-e1ffb79ddf)	Vulnerability - level 4	Vuln
283736	Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2023-a5564c0a3f)	Vulnerability - level 4	Vuln
283759	Fedora Security Update for edk2 (FEDORA-2023-e821b64a4c)	Vulnerability - level 4	Vuln
283844	Fedora Security Update for libldb (FEDORA-2023-fca3bfed78)	Vulnerability - level 4	Vuln
283895	Fedora Security Update for libldb (FEDORA-2023-1c172e3264)	Vulnerability - level 3	Vuln
283901	Fedora Security Update for lldpd (FEDORA-2023-c0c184a019)	Vulnerability - level 4	Vuln
283902	Fedora Security Update for lldpd (FEDORA-2023-3e4feeadece)	Vulnerability - level 4	Vuln
284191	Fedora Security Update for lldpd (FEDORA-2023-88991d2713)	Vulnerability - level 4	Vuln
284210	Fedora Security Update for libldb (FEDORA-2023-7ac413b969)	Vulnerability - level 3	Vuln
284299	Fedora Security Update for etcd (FEDORA-2022-28d38313c8)	Vulnerability - level 5	Vuln
296002	Solaris 11.3 Support Repository Update (SRU) 9.4.0 Missing	Vulnerability - level 4	Vuln
296003	Solaris 11.3 Support Repository Update (SRU) 10.5.0 Missing	Vulnerability - level 4	Vuln
296020	Solaris 11.3 Support Repository Update (SRU) 28.4.0 Missing	Vulnerability - level 4	Vuln
296021	Oracle Solaris 10 Multiple Vulnerabilities (Third Party Bulletin - January 2018)	Vulnerability - level 4	Vuln
296029	Solaris 11.3 Support Repository Update (SRU) 35.6.0 Missing	Vulnerability - level 4	Vuln
296050	Oracle Solaris 11.3 Support Repository Update (SRU) 36.24.0 Missing (CPUJAN2021)	Vulnerability - level 3	Vuln
296051	Oracle Solaris 11.4 Support Repository Update (SRU) 30.88.3 Missing (CPUJAN2021)	Vulnerability - level 4	Vuln
296053	Oracle Solaris 11.4 Support Repository Update (SRU) 35.94.4 Missing (CPUJUL2021)	Vulnerability - level 4	Vuln
296056	Oracle Solaris 11.4 Support Repository Update (SRU) 44.113.4 Missing (CPUAPR2022)	Vulnerability - level 4	Vuln
296059	Oracle Solaris 11.4 Support Repository Update (SRU) 36.0.1.101.2 Missing (CPUJUL2021)	Vulnerability - level 3	Vuln
296060	Oracle Solaris 11.4 Support Repository Update (SRU) 37.0.1.101.1 Missing (CPUJUL2021)	Vulnerability - level 3	Vuln
296061	Oracle Solaris 11.4 Support Repository Update (SRU) 42.113.1 Missing (CPUJAN2022)	Vulnerability - level 4	Vuln
296063	Oracle Solaris 11.4 Support Repository Update (SRU) 45.119.2 Missing (CPUAPR2022)	Vulnerability - level 3	Vuln
296065	Oracle Solaris 11.4 Support Repository Update (SRU) 39.107.1 Missing (CPUOCT2021)	Vulnerability - level 3	Vuln
296066	Oracle Solaris 11.4 Support Repository Update (SRU) 40.107.3 Missing (CPUOCT2021)	Vulnerability - level 3	Vuln
296067	Oracle Solaris 11.4 Support Repository Update (SRU) 33.94.0 Missing (CPUAPR2021)	Vulnerability - level 3	Vuln
296068	Oracle Solaris 11.4 Support Repository Update (SRU) 34.94.4 Missing (CPUAPR2021)	Vulnerability - level 3	Vuln
296069	Oracle Solaris 11.4 Support Repository Update (SRU) 31.88.5 Missing (CPUJAN2021)	Vulnerability - level 3	Vuln
296072	Oracle Solaris 11.4 Support Repository Update (SRU) 25.75.3 Missing (CPUJUL2020)	Vulnerability - level 3	Vuln

296073	Oracle Solaris 11.4 Support Repository Update (SRU) 24.75.2 Missing (CPUJUL2020)	Vulnerability - level 3	Vuln
296074	Oracle Solaris 11.4 Support Repository Update (SRU) 22.69.4 Missing (CPUAPR2020)	Vulnerability - level 3	Vuln
296075	Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)	Vulnerability - level 3	Vuln
296078	Oracle Solaris 11.4 Support Repository Update (SRU) 16.4.0 Missing (CPUOCT2019)	Vulnerability - level 3	Vuln
296081	Oracle Solaris 11.4 Support Repository Update (SRU) 12.5.0 Missing (CPUJUL2019)	Vulnerability - level 3	Vuln
296082	Oracle Solaris 11.4 Support Repository Update (SRU) 48.126.1 Missing (CPUJUL2022)	Vulnerability - level 3	Vuln
296083	Oracle Solaris 11.4 Support Repository Update (SRU) 49.126.2 Missing (CPUJUL2022)	Vulnerability - level 4	Vuln
296084	Oracle Solaris 11.4 Support Repository Update (SRU) 50.126.3 Missing (CPUOCT2022)	Vulnerability - level 4	Vuln
296085	Oracle Solaris 11.3 Support Repository Update (SRU) 36.30.0 Missing (CPUOCT2022)	Vulnerability - level 4	Vuln
296088	Oracle Solaris 11.4 Support Repository Update (SRU) 9.1.5 Missing (CPUAPR2019)	Vulnerability - level 5	Vuln
296091	Oracle Solaris 11.4 Support Repository Update (SRU) 6.1.4 Missing (CPUJAN2019)	Vulnerability - level 5	Vuln
296092	Oracle Solaris 11.4 Support Repository Update (SRU) 7.1.4 Missing (CPUJAN2019)	Vulnerability - level 5	Vuln
296095	Oracle Solaris 11.4 Support Repository Update (SRU) 54.138.1 Missing (CPUJAN2023)	Vulnerability - level 2	Vuln
296098	Oracle Solaris 11.4 Support Repository Update (SRU) 52.132.2 Missing (CPUOCT2022)	Vulnerability - level 4	Vuln
296099	Oracle Solaris 11.4 Support Repository Update (SRU) 57.144.3 Missing (CPUAPR2023)	Vulnerability - level 4	Vuln
316002	Cisco IOS Network Time Protocol Daemon Multiple Vulnerabilities (cisco-sa-20160603-ntpd)	Vulnerability - level 3	Practice
316007	Cisco IOS and IOS XE IPv6 Neighbor Discovery Crafted Packet Denial of Service Vulnerability (cisco-sa-20160525-ipv6)	Vulnerability - level 3	Practice
316008	Cisco NX-OS IPv6 Neighbor Discovery Crafted Packet Denial of Service Vulnerability (cisco-sa-20160525-ipv6)	Vulnerability - level 3	Vuln
316009	Cisco ASA IPv6 Neighbor Discovery Crafted Packet Denial of Service Vulnerability (cisco-sa-20160525-ipv6)	Vulnerability - level 3	Vuln
316015	Cisco Nexus ntpd multiple vulnerabilities (cisco-sa-20160428-ntpd)	Vulnerability - level 3	Vuln
316016	Cisco ASA OpenSSL Multiple Vulnerabilities (cisco-sa-20160504-openssl)	Vulnerability - level 3	Vuln
316017	Cisco Nexus OpenSSL Multiple Vulnerabilities (cisco-sa-20160504-openssl)	Vulnerability - level 3	Vuln
316022	Cisco IOS and IOS XE Software Internet Key Exchange Version 1 Fragmentation Denial of Service Vulnerability (cisco-sa-20160928-ios-ikev1)	Vulnerability - level 4	Practice
316032	Cisco IOS and IOS XE Software AAA Login Denial of Service Vulnerability (cisco-sa-20160928-aaados)	Vulnerability - level 4	Practice
316034	Cisco IOS and IOS XE Software DNS Forwarder Denial of Service Vulnerability (cisco-sa-20160928-dns)	Vulnerability - level 4	Practice
316037	Cisco IOS and IOS XE Software H.323 Message Validation Denial of Service Vulnerability(cisco-sa-20160928-h323)	Vulnerability - level 4	Practice
316038	Cisco IOS and IOS XE Software Multicast Routing Denial of Service Vulnerabilities (cisco-sa-20160928-msdp)	Vulnerability - level 4	Practice
316039	Cisco IOS and IOS XE Software Smart Install Memory Leak Vulnerability (cisco-sa-20160928-smi)	Vulnerability - level 4	Practice
316040	Cisco NX-OS OpenSSL Multiple Vulnerabilities (cisco-sa-20160927-openssl)	Potential Vulnerability - level 3	Practice

316066	Cisco Nexus Network Time Protocol Daemon Multiple Vulnerabilities (cisco-sa-20161123-ntpd)	Vulnerability - level 3	Vuln
316103	Cisco ASA OpenSSL Multiple Vulnerabilities (cisco-sa-20150612-openssl)	Vulnerability - level 4	Vuln
316122	Cisco NX-OS Network Time Protocol Daemon Multiple Vulnerabilities (cisco-sa-20160603-ntpd)	Vulnerability - level 4	Vuln
316125	Cisco IOS and IOS XE Software SNMP Remote Code Execution (RCE) Vulnerabilities (cisco-sa-20170629-snmp)	Vulnerability - level 4	Practice
316176	Cisco Unified Communications Manager OpenSSH X11 Forwarding Vulnerability (CSCuz61569)	Vulnerability - level 3	Vuln
316240	Cisco Adaptive Security Appliance TLS Denial of Service Vulnerability (cisco-sa-20180418-asa3)	Vulnerability - level 4	Vuln
316241	Cisco Adaptive Security Appliance Application Layer Protocol Inspection Denial of Service Vulnerabilities(cisco-sa-20180418-asa_inspect)	Vulnerability - level 4	Vuln
316243	Cisco Adaptive Security Appliance Flow Creation Denial of Service Vulnerability(cisco-sa-20180418-asa2)	Vulnerability - level 4	Vuln
316244	Cisco Adaptive Security Appliance (ASA) Virtual Private Network (VPN) Secure Sockets Layer (SSL) Client Certificate Bypass Vulnerability (cisco-sa-20180418-asa1)	Vulnerability - level 4	Vuln
316266	Cisco NX-OS CPU Side-Channel Information Disclosure Vulnerabilities (cisco-sa-20180521-cpusidechannel)	Vulnerability - level 3	Vuln
316318	Cisco IOS and IOS XE Software OSPFv3 Denial of Service Vulnerability(cisco-sa-20180926-ospfv3-dos)	Vulnerability - level 4	Practice
316319	Cisco IOS XE Software HTTP Denial of Service Vulnerability(cisco-sa-20180926-webdos)	Vulnerability - level 4	Practice
316320	Cisco IOS Software Precision Time Protocol Denial of Service Vulnerability(cisco-sa-20180926-ptp)	Vulnerability - level 4	Practice
316321	Cisco IOS XE Software and Cisco ASA 5500-X Series Adaptive Security Appliance IPsec Denial of Service Vulnerability(cisco-sa-20180926-ipsec)	Vulnerability - level 4	Practice
316327	Cisco IOS and IOS XE Software IPv6 Hop-by-Hop Options Denial of Service Vulnerability(cisco-sa-20180926-ipv6hbh)	Vulnerability - level 4	Practice
316333	Cisco IOS and IOS XE Software Plug and Play Agent Memory Leak Vulnerability(cisco-sa-20180926-pnp-memleak)	Vulnerability - level 3	Practice
316334	Cisco IOS and IOS XE Software Cisco Discovery Protocol Denial of Service Vulnerability(cisco-sa-20180926-cdp-dos)	Vulnerability - level 3	Practice
316362	Cisco UCS 6200 Series Fabric Interconnects Multiple Vulnerabilities in Network Time Protocol Daemon (CSCuz44156)	Vulnerability - level 3	Vuln
316384	Cisco Unity Express Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (cisco-sa-20160927-openssl)	Vulnerability - level 4	Vuln
316454	Cisco ASA Secure Boot Hardware Tampering Vulnerability(cisco-sa-20190513-secureboot)	Vulnerability - level 4	Vuln
316455	Cisco NX-OS Secure Boot Hardware Tampering Vulnerability(cisco-sa-20190513-secureboot)(CSCvn77245,CSCvn77141,CSCvn77143,CSCvn77142)	Vulnerability - level 4	Vuln
316484	Cisco ASR 1001-X , ASR 1002-HX Secure Boot Hardware Tampering Vulnerability(cisco-sa-20190513-secureboot)(CSCvn77166,CSCvn89145)	Vulnerability - level 4	Vuln
316594	Multiple Vulnerabilities in Open Secure Sockets Layer (OpenSSL) Affecting Cisco Products (cisco-sa-20150320-openssl)	Vulnerability - level 4	Vuln
316625	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability(cisco-sa-webui-PZgQxjfg)	Vulnerability - level 4	Practice
316626	Cisco IOS and IOS XE Software Secure Shell Denial of Service Vulnerability(cisco-sa-ssh-dos-Un22sd2A)	Vulnerability - level 4	Practice
316629	Cisco IOS XE Software Web UI Command Injection Vulnerability(cisco-sa-web-cmdinj4-S2TmH7GA)	Vulnerability - level 4	Practice
316631	Cisco IOS XE Software Digital Signature Verification Bypass Vulnerability(cisco-sa-iosxe-digsig-bypass-FYQ3bmVq)	Vulnerability - level 4	Practice

316634	Cisco IOS XE Software Web UI Remote Code Execution Vulnerability(cisco-sa-iosxe-webui-rce-uk8BXcUD)	Vulnerability - level 4	Practice
316641	Cisco IOS XE Software Web UI Command Injection Vulnerability(cisco-sa-web-cmdinj2-fOnjk2LD)	Vulnerability - level 4	Practice
316761	Cisco IOS XE Software Web UI Improper Input Validation Vulnerability(cisco-sa-WEB-UI-exNFmcPO)	Vulnerability - level 3	Practice
316898	Cisco IOS XE Software DECnet Phase IV/OSI Denial of Service (DoS) Vulnerability(cisco-sa-iosxe-decnet-dos-cuPWDkYL)	Vulnerability - level 3	Practice
316899	Cisco IOS XE Software Web UI Cross-Site WebSocket Hijacking Vulnerability(cisco-sa-iosxe-cswsh-FKk9AzT5)	Vulnerability - level 3	Practice
316900	Cisco IOS XE Software Plug-and-Play Privilege Escalation Vulnerability(cisco-sa-ios-xe-pnp-priv-esc-AmG3kuVL)	Vulnerability - level 3	Practice
316902	Cisco IOS XE Software DNS NAT Protocol Application Layer Gateway Denial of Service Vulnerability(cisco-sa-alg-dos-hbBS7SZE)	Vulnerability - level 3	Practice
316905	Cisco IOS and IOS XE Software Common Industrial Protocol Privilege Escalation Vulnerability(cisco-sa-XE-SAP-OPLbze68)	Vulnerability - level 3	Practice
316908	Cisco IOS XE Software Web UI Denial of Service Vulnerabilities(cisco-sa-xe-webui-dos-z9yqYQAn)	Vulnerability - level 3	Practice
316911	Cisco IOS XE Software Web UI OS Command Injection Vulnerability(cisco-sa-ios-xe-os-cmd-inj-Ef6TV5e9)	Vulnerability - level 3	Practice
316994	Cisco Internetwork Operating System (IOS-XE) Vulnerability in Open Secure Sockets Layer (OpenSSL) Affecting Cisco Products (cisco-sa-openssl-2021-GHY28dJd)	Potential Vulnerability - level 3	Practice
316995	Cisco Nexus Operating System (NX-OS) Vulnerability in Open Secure Sockets Layer (OpenSSL) Affecting Cisco Products (cisco-sa-openssl-2021-GHY28dJd)	Potential Vulnerability - level 3	Practice
316996	Cisco Web Security Appliance Denial of Service (DOS) Vulnerability in Open Secure Sockets Layer (OpenSSL) Affecting Cisco Products (cisco-sa-openssl-2021-GHY28dJd)	Vulnerability - level 3	Vuln
330001	IBM AIX NTP Multiple Vulnerabilities	Vulnerability - level 3	Vuln
330004	IBM AIX OpenSSL Multiple Vulnerabilities	Vulnerability - level 4	Vuln
330007	IBM AIX NTP Multiple Vulnerabilities (ntp_advisory7.asc)	Vulnerability - level 3	Vuln
330009	IBM AIX OpenSSH Multiple Vulnerabilities (openssh_advisory9)	Vulnerability - level 4	Vuln
330012	IBM AIX OpenSSL Multiple Vulnerabilities (openssl_advisory21)	Vulnerability - level 3	Vuln
330021	IBM AIX OpenSSH Multiple Vulnerabilities (openssh_advisory10)	Vulnerability - level 3	Vuln
330028	IBM AIX NTP Multiple Vulnerabilities (ntp_advisory9.asc)	Vulnerability - level 4	Vuln
330029	IBM AIX Java Multiple Vulnerabilities (java_july2017_advisory)	Vulnerability - level 4	Vuln
330034	IBM AIX OpenSSH Vulnerability (openssh_advisory11)	Vulnerability - level 3	Vuln
330036	IBM AIX OpenSSL Security Bypass Vulnerability (openssl_advisory24)	Vulnerability - level 3	Vuln
330037	IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Security Bypass Vulnerability (openssl_advisory25)	Vulnerability - level 3	Vuln
330048	IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Transport Layer Security (TLS) Handshake Denial Of Service (DoS) Vulnerability (openssl_advisory28)	Vulnerability - level 3	Vuln
330066	IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Information Disclosure Vulnerability (openssl_advisory31)	Vulnerability - level 3	Vuln
330079	IBM Advanced Interactive eXecutive (AIX) Multiple Vulnerabilities in Open Secure Sockets Layer (OpenSSL) (openssl_advisory32)	Vulnerability - level 3	Vuln
330081	IBM Advanced Interactive eXecutive (AIX) Multiple Vulnerabilities in Open Secure Sockets Layer (OpenSSL) (openssl_advisory33)	Vulnerability - level 2	Vuln
330085	IBM AIX BIND Denial of Service Vulnerability (bind_advisory19)	Vulnerability - level 3	Vuln

330091	IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Out-Of-Bounds Vulnerability (openssl_advisory34)	Vulnerability - level 3	Vuln
330098	IBM AIX BIND Denial of Service (DoS) Vulnerability (bind_advisory20)	Vulnerability - level 3	Vuln
330108	IBM AIX Domain Name System (DNS) cache poisoning Vulnerability due to ISC BIND (bind_advisory21)	Vulnerability - level 4	Vuln
330109	IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Arbitrary Code Execution Vulnerability (openssl_advisory36)	Vulnerability - level 4	Vuln
330124	IBM AIX Multiple Vulnerabilities in Python (python_advisory)	Vulnerability - level 5	Vuln
330133	IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory38)	Vulnerability - level 4	Vuln
350006	Amazon Linux Security Advisory for openssl: ALAS-2016-695	Vulnerability - level 4	Vuln
350021	Amazon Linux Security Advisory for openssl098e: ALAS-2016-682	Vulnerability - level 4	Vuln
350022	Amazon Linux Security Advisory for tomcat6: ALAS-2016-681	Vulnerability - level 3	Vuln
350023	Amazon Linux Security Advisory for tomcat7: ALAS-2016-680	Vulnerability - level 3	Vuln
350024	Amazon Linux Security Advisory for tomcat8: ALAS-2016-679	Vulnerability - level 3	Vuln
350028	Amazon Linux Security Advisory for openssh: ALAS-2016-675	Vulnerability - level 3	Vuln
350042	Amazon Linux Security Advisory for openssl: ALAS-2016-661	Vulnerability - level 4	Vuln
350044	Amazon Linux Security Advisory for tomcat8: ALAS-2016-658	Vulnerability - level 3	Vuln
350045	Amazon Linux Security Advisory for tomcat7: ALAS-2016-657	Vulnerability - level 3	Vuln
350053	Amazon Linux Security Advisory for ntp: ALAS-2016-649	Vulnerability - level 4	Vuln
350077	Amazon Linux Security Advisory for openssh: ALAS-2015-625	Vulnerability - level 3	Vuln
350088	Amazon Linux Security Advisory for openssl: ALAS-2015-614	Vulnerability - level 3	Vuln
350095	Amazon Linux Security Advisory for ntp: ALAS-2015-607	Vulnerability - level 4	Vuln
350098	Amazon Linux Security Advisory for libwmf: ALAS-2015-604	Vulnerability - level 4	Vuln
350107	Amazon Linux Security Advisory for jakarta-taglibs-standard: ALAS-2015-595	Vulnerability - level 4	Vuln
350109	Amazon Linux Security Advisory for ntp: ALAS-2015-593	Vulnerability - level 2	Vuln
350110	Amazon Linux Security Advisory for openssh: ALAS-2015-592	Vulnerability - level 3	Vuln
350115	Amazon Linux Security Advisory for subversion,mod_dav_svn: ALAS-2015-587	Vulnerability - level 3	Vuln
350116	Amazon Linux Security Advisory for java-1.6.0-openjdk: ALAS-2015-586	Vulnerability - level 4	Vuln
350125	Amazon Linux Security Advisory for libgcrypt: ALAS-2015-577	Vulnerability - level 3	Vuln
350126	Amazon Linux Security Advisory for tigervnc: ALAS-2015-576	Vulnerability - level 3	Vuln
350131	Amazon Linux Security Advisory for java-1.8.0-openjdk: ALAS-2015-571	Vulnerability - level 4	Vuln
350132	Amazon Linux Security Advisory for java-1.7.0-openjdk: ALAS-2015-570	Vulnerability - level 5	Vuln
350133	Amazon Linux Security Advisory for nss,nss-util: ALAS-2015-569	Vulnerability - level 3	Vuln
350134	Amazon Linux Security Advisory for openssh: ALAS-2015-568	Vulnerability - level 3	Vuln
350147	Amazon Linux Security Advisory for mod_dav_svn,subversion: ALAS-2015-555	Vulnerability - level 3	Vuln
350152	Amazon Linux Security Advisory for openssl: ALAS-2015-550	Vulnerability - level 3	Vuln
350153	Amazon Linux Security Advisory for ruby22: ALAS-2015-549	Vulnerability - level 3	Vuln
350154	Amazon Linux Security Advisory for ruby21: ALAS-2015-548	Vulnerability - level 3	Vuln
350155	Amazon Linux Security Advisory for ruby20: ALAS-2015-547	Vulnerability - level 3	Vuln
350175	Amazon Linux Security Advisory for tomcat8: ALAS-2015-527	Vulnerability - level 3	Vuln
350176	Amazon Linux Security Advisory for tomcat7: ALAS-2015-526	Vulnerability - level 3	Vuln
350177	Amazon Linux Security Advisory for tomcat6: ALAS-2015-525	Vulnerability - level 3	Vuln
350182	Amazon Linux Security Advisory for ntp: ALAS-2015-520	Vulnerability - level 4	Vuln
350204	Amazon Linux Security Advisory for openssl: ALAS-2015-498	Vulnerability - level 3	Vuln
350206	Amazon Linux Security Advisory for ntp: ALAS-2015-496	Vulnerability - level 3	Vuln
350225	Amazon Linux Security Advisory for curl: ALAS-2015-477	Vulnerability - level 3	Vuln
350233	Amazon Linux Security Advisory for openssl: ALAS-2015-469	Vulnerability - level 3	Vuln
350236	Amazon Linux Security Advisory for jasper: ALAS-2015-466	Vulnerability - level 4	Vuln
350247	Amazon Linux Security Advisory for kernel: ALAS-2014-455	Vulnerability - level 3	Vuln

350248	Amazon Linux Security Advisory for docker: ALAS-2014-454	Vulnerability - level 5	Vuln
350258	Amazon Linux Security Advisory for openssl: AL2012-2014-003	Vulnerability - level 4	Vuln
350259	Amazon Linux Security Advisory for ntp: AL2012-2016-109	Vulnerability - level 4	Vuln
350265	Amazon Linux Security Advisory for mysql56: ALAS-2016-701	Vulnerability - level 5	Vuln
350272	Amazon Linux Security Advisory for ntp: ALAS-2016-708	Vulnerability - level 3	Vuln
350313	Amazon Linux Security Advisory for json-c: ALAS-2014-416	Vulnerability - level 3	Vuln
350319	Amazon Linux Security Advisory for jakarta-commons-httpclient: ALAS-2014-410	Vulnerability - level 4	Vuln
350338	Amazon Linux Security Advisory for openssl: ALAS-2014-391	Vulnerability - level 3	Vuln
350380	Amazon Linux Security Advisory for openssl: ALAS-2014-349	Vulnerability - level 4	Vuln
350384	Amazon Linux Security Advisory for elfutils: ALAS-2014-345	Vulnerability - level 3	Vuln
350385	Amazon Linux Security Advisory for tomcat6: ALAS-2014-344	Vulnerability - level 3	Vuln
350401	Amazon Linux Security Advisory for ntp: AL2012-2016-102	Vulnerability - level 4	Vuln
350402	Amazon Linux Security Advisory for openssl: AL2012-2016-101	Vulnerability - level 3	Vuln
350403	Amazon Linux Security Advisory for curl: ALAS-2014-322	Vulnerability - level 3	Vuln
350410	Amazon Linux Security Advisory for openssl: ALAS-2014-320	Vulnerability - level 5	Vuln
350421	Amazon Linux Security Advisory for java-1.6.0-openjdk: AL2012-2015-090	Vulnerability - level 4	Vuln
350424	Amazon Linux Security Advisory for ntp: AL2012-2015-087	Vulnerability - level 3	Vuln
350437	Amazon Linux Security Advisory for nginx: ALAS-2014-308	Vulnerability - level 4	Vuln
350438	Amazon Linux Security Advisory for libtiff: ALAS-2014-307	Vulnerability - level 3	Vuln
350442	Amazon Linux Security Advisory for openswan: ALAS-2014-303	Vulnerability - level 3	Vuln
350444	Amazon Linux Security Advisory for gnutls: ALAS-2014-301	Vulnerability - level 4	Vuln
350447	Amazon Linux Security Advisory for mysql51: ALAS-2014-298	Vulnerability - level 3	Vuln
350456	Amazon Linux Security Advisory for kernel: ALAS-2014-289	Vulnerability - level 3	Vuln
350466	Amazon Linux Security Advisory for gnupg: ALAS-2014-278	Vulnerability - level 3	Vuln
350471	Amazon Linux Security Advisory for openssl: ALAS-2014-273	Vulnerability - level 4	Vuln
350475	Amazon Linux Security Advisory for subversion: ALAS-2013-269	Vulnerability - level 3	Vuln
350477	Amazon Linux Security Advisory for libjpeg-turbo: ALAS-2013-267	Vulnerability - level 3	Vuln
350484	Amazon Linux Security Advisory for xorg-x11-server: ALAS-2013-260	Vulnerability - level 2	Vuln
350489	Amazon Linux Security Advisory for 389-ds-base: ALAS-2013-255	Vulnerability - level 4	Vuln
350490	Amazon Linux Security Advisory for mod24_nss: ALAS-2013-254	Vulnerability - level 3	Vuln
350491	Amazon Linux Security Advisory for mod_nss: ALAS-2013-253	Vulnerability - level 3	Vuln
350500	Amazon Linux Security Advisory for postgresql8: ALAS-2013-244	Vulnerability - level 3	Vuln
350507	Amazon Linux Security Advisory for gnupg2: ALAS-2013-237	Vulnerability - level 3	Vuln
350508	Amazon Linux Security Advisory for gnupg: ALAS-2013-236	Vulnerability - level 3	Vuln
350514	Amazon Linux Security Advisory for rubygems: ALAS-2013-230	Vulnerability - level 3	Vuln
350523	Amazon Linux Security Advisory for subversion: ALAS-2013-221	Vulnerability - level 3	Vuln
350526	Amazon Linux Security Advisory for kernel: ALAS-2013-218	Vulnerability - level 3	Vuln
350529	Amazon Linux Security Advisory for haproxy: ALAS-2013-215	Vulnerability - level 3	Vuln
350536	Amazon Linux Security Advisory for krb5: ALAS-2013-208	Vulnerability - level 3	Vuln
350538	Amazon Linux Security Advisory for php54: ALAS-2013-206	Vulnerability - level 5	Vuln
350539	Amazon Linux Security Advisory for php: ALAS-2013-205	Vulnerability - level 5	Vuln
350551	Amazon Linux Security Advisory for ruby19: ALAS-2013-195	Vulnerability - level 3	Vuln
350552	Amazon Linux Security Advisory for httpd24: ALAS-2013-194	Vulnerability - level 3	Vuln
350553	Amazon Linux Security Advisory for httpd: ALAS-2013-193	Vulnerability - level 3	Vuln
350558	Amazon Linux Security Advisory for libxml2: ALAS-2013-188	Vulnerability - level 3	Vuln
350561	Amazon Linux Security Advisory for java-1.6.0-openjdk: ALAS-2013-185	Vulnerability - level 4	Vuln
350563	Amazon Linux Security Advisory for java-1.7.0-openjdk: ALAS-2013-183	Vulnerability - level 5	Vuln
350566	Amazon Linux Security Advisory for subversion: ALAS-2013-180	Vulnerability - level 3	Vuln
350568	Amazon Linux Security Advisory for postgresql9: ALAS-2013-178	Vulnerability - level 5	Vuln
350569	Amazon Linux Security Advisory for perl: ALAS-2013-177	Vulnerability - level 3	Vuln
350570	Amazon Linux Security Advisory for bind: ALAS-2013-176	Vulnerability - level 4	Vuln
350571	Amazon Linux Security Advisory for httpd24: ALAS-2013-175	Vulnerability - level 3	Vuln
350572	Amazon Linux Security Advisory for httpd: ALAS-2013-174	Vulnerability - level 3	Vuln
350573	Amazon Linux Security Advisory for ruby: ALAS-2013-173	Vulnerability - level 3	Vuln

350575	Amazon Linux Security Advisory for openssl: ALAS-2013-171	Vulnerability - level 3	Vuln
350583	Amazon Linux Security Advisory for java-1.6.0-openjdk: ALAS-2013-163	Vulnerability - level 4	Vuln
350584	Amazon Linux Security Advisory for java-1.7.0-openjdk: ALAS-2013-162	Vulnerability - level 4	Vuln
350600	Amazon Linux Security Advisory for libtiff: ALAS-2012-147	Vulnerability - level 3	Vuln
350607	Amazon Linux Security Advisory for libproxy: ALAS-2012-140	Vulnerability - level 3	Vuln
350616	Amazon Linux Security Advisory for freeradius: ALAS-2012-131	Vulnerability - level 3	Vuln
350621	Amazon Linux Security Advisory for libexif: ALAS-2012-126	Vulnerability - level 3	Vuln
350624	Amazon Linux Security Advisory for libxslt: ALAS-2012-123	Vulnerability - level 4	Vuln
350628	Amazon Linux Security Advisory for java-1.6.0-openjdk: ALAS-2012-119	Vulnerability - level 4	Vuln
350638	Amazon Linux Security Advisory for glibc: ALAS-2012-109	Vulnerability - level 3	Vuln
350699	Amazon Linux Security Advisory for texlive: ALAS-2012-048	Vulnerability - level 3	Vuln
350707	Amazon Linux Security Advisory for t1lib: ALAS-2012-040	Vulnerability - level 3	Vuln
350721	Amazon Linux Security Advisory for kernel: ALAS-2011-026	Vulnerability - level 3	Vuln
350751	Amazon Linux Security Advisory for openssl: AL2012-2015-081	Vulnerability - level 3	Vuln
350756	Amazon Linux Security Advisory for tomcat-native: AL2012-2015-076	Vulnerability - level 3	Vuln
350757	Amazon Linux Security Advisory for tomcat6: AL2012-2015-075	Vulnerability - level 3	Vuln
350764	Amazon Linux Security Advisory for libtiff: AL2012-2015-068	Vulnerability - level 3	Vuln
350769	Amazon Linux Security Advisory for tomcat7: AL2012-2015-062	Vulnerability - level 3	Vuln
350772	Amazon Linux Security Advisory for openssl: AL2012-2015-059	Vulnerability - level 3	Vuln
350784	Amazon Linux Security Advisory for openswan: AL2012-2015-047	Vulnerability - level 3	Vuln
350791	Amazon Linux Security Advisory for gnutls: AL2012-2015-040	Vulnerability - level 3	Vuln
350798	Amazon Linux Security Advisory for openssl: AL2012-2015-033	Vulnerability - level 3	Vuln
350799	Amazon Linux Security Advisory for subversion: AL2012-2015-032	Vulnerability - level 3	Vuln
350809	Amazon Linux Security Advisory for jasper: AL2012-2015-022	Vulnerability - level 3	Vuln
350814	Amazon Linux Security Advisory for bind: AL2012-2015-017	Vulnerability - level 3	Vuln
350817	Amazon Linux Security Advisory for mod_nss: AL2012-2014-014	Vulnerability - level 3	Vuln
350828	Amazon Linux Security Advisory for openssl: AL2012-2016-110	Vulnerability - level 3	Vuln
350836	Amazon Linux Security Advisory for jakarta-taglibs-standard: AL2012-2016-118	Vulnerability - level 3	Vuln
350839	Amazon Linux Security Advisory for tomcat7: AL2012-2016-121	Vulnerability - level 3	Vuln
350843	Amazon Linux Security Advisory for openssl098e: AL2012-2016-125	Vulnerability - level 3	Vuln
350850	Amazon Linux Security Advisory for openssh: AL2012-2016-133	Vulnerability - level 3	Vuln
350855	Amazon Linux Security Advisory for tomcat6,tomcat7,tomcat8: ALAS-2016-722	Vulnerability - level 3	Vuln
350858	Amazon Linux Security Advisory for httpd24,httpd: ALAS-2016-725	Vulnerability - level 4	Vuln
350860	Amazon Linux Security Advisory for openssl: AL2012-2016-136	Vulnerability - level 3	Vuln
350863	Amazon Linux Security Advisory for kernel: ALAS-2016-726	Vulnerability - level 3	Vuln
350864	Amazon Linux Security Advisory for ntp: ALAS-2016-727	Vulnerability - level 3	Vuln
350865	Amazon Linux Security Advisory for php55,php56: ALAS-2016-728	Vulnerability - level 3	Vuln
350869	Amazon Linux Security Advisory for curl: ALAS-2016-730	Vulnerability - level 3	Vuln
350881	Amazon Linux Security Advisory for httpd: AL2012-2016-139	Vulnerability - level 3	Vuln
350884	Amazon Linux Security Advisory for ntp: AL2012-2016-142	Vulnerability - level 3	Vuln
350894	Amazon Linux Security Advisory for tomcat7: AL2012-2016-147	Vulnerability - level 3	Vuln
350899	Amazon Linux Security Advisory for ntp: AL2012-2016-152	Vulnerability - level 3	Vuln
350904	Amazon Linux Security Advisory for openvpn: ALAS-2016-750	Vulnerability - level 3	Vuln
350910	Amazon Linux Security Advisory for openssl: ALAS-2016-755	Vulnerability - level 3	Vuln
350921	Amazon Linux Security Advisory for curl: ALAS-2016-766	Vulnerability - level 3	Vuln
350928	Amazon Linux Security Advisory for openssh: ALAS-2016-770	Vulnerability - level 3	Vuln
350939	Amazon Linux Security Advisory for ntp: ALAS-2017-781	Vulnerability - level 3	Vuln
350964	Amazon Linux Security Advisory for curl: ALAS-2017-806	Vulnerability - level 2	Vuln
350969	Amazon Linux Security Advisory for kernel: ALAS-2017-811	Vulnerability - level 4	Vuln
350972	Amazon Linux Security Advisory for tomcat7: AL2012-2017-161	Vulnerability - level 3	Vuln
350981	Amazon Linux Security Advisory for ntp: ALAS-2017-816	Vulnerability - level 3	Vuln
351032	Amazon Linux Security Advisory for ntp: AL2012-2017-176	Vulnerability - level 3	Vuln

351035	Amazon Linux Security Advisory for ntp: AL2012-2017-179	Vulnerability - level 3	Vuln
351048	Amazon Linux Security Advisory for java-1.8.0-openjdk: ALAS-2017-860	Vulnerability - level 5	Vuln
351057	Amazon Linux Security Advisory for java-1.7.0-openjdk: ALAS-2017-869	Vulnerability - level 5	Vuln
351094	Amazon Linux Security Advisory for mercurial: ALAS-2017-893	Vulnerability - level 4	Vuln
351139	Amazon Linux Security Advisory for mercurial: AL2012-2017-220	Vulnerability - level 4	Vuln
351151	Amazon Linux Security Advisory for java-1.7.0-openjdk: ALAS-2017-936	Vulnerability - level 5	Vuln
351156	Amazon Linux Security Advisory for kernel: AL2012-2017-222	Vulnerability - level 3	Vuln
351179	Amazon Linux Security Advisory for quagga: ALAS-2018-957	Vulnerability - level 4	Vuln
351247	Amazon Linux Security Advisory for quagga: AL2012-2018-235	Vulnerability - level 3	Vuln
351253	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS-2018-1016	Vulnerability - level 3	Vuln
351255	Amazon Linux Security Advisory for openssh: ALAS-2018-1018	Vulnerability - level 3	Vuln
351276	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-2018-1004	Vulnerability - level 3	Vuln
351281	Amazon Linux Security Advisory for ntp: ALAS2-2018-1009	Vulnerability - level 3	Vuln
351304	Amazon Linux Security Advisory for openssh: ALAS2-2018-1042	Vulnerability - level 2	Vuln
351319	Amazon Linux Security Advisory for kernel: ALAS-2018-1049 (SegmentSmack)	Vulnerability - level 5	Vuln
351320	Amazon Linux Security Advisory for kernel: ALAS2-2018-1050 (SegmentSmack)	Vulnerability - level 5	Vuln
351322	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): AL2012-2018-245	Vulnerability - level 3	Vuln
351329	Amazon Linux Security Advisory for kernel: ALAC2012-2018-005	Vulnerability - level 3	Vuln
351331	Amazon Linux Security Advisory for kernel: ALAC2012-2018-007 (SegmentSmack/FragmentSmack)	Vulnerability - level 3	Vuln
351333	Amazon Linux Security Advisory for tomcat7,tomcat80: ALAS-2018-1055	Vulnerability - level 4	Vuln
351334	Amazon Linux Security Advisory for tomcat8: ALAS-2018-1056	Vulnerability - level 4	Vuln
351355	Amazon Linux Security Advisory for tomcat7: AL2012-2018-254	Vulnerability - level 3	Vuln
351358	Amazon Linux Security Advisory for kernel: ALAC2012-2018-008	Vulnerability - level 3	Vuln
351382	Amazon Linux Security Advisory for openssh: AL2012-2018-261	Vulnerability - level 3	Vuln
351406	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS-2018-1098	Vulnerability - level 3	Vuln
351419	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-2018-1102	Vulnerability - level 3	Vuln
351425	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS-2018-1102	Vulnerability - level 3	Vuln
351432	Amazon Linux Security Advisory for curl: ALAS-2018-1112	Vulnerability - level 2	Vuln
351443	Amazon Linux Security Advisory for wpa_supplicant: ALAS2-2018-1122	Vulnerability - level 3	Vuln
351445	Amazon Linux Security Advisory for xerces-c: ALAS2-2018-1124	Vulnerability - level 3	Vuln
351446	Amazon Linux Security Advisory for kernel: ALAC2012-2018-012	Vulnerability - level 3	Vuln
351449	Amazon Linux Security Advisory for kernel: ALAC2012-2018-015 - DEPRECATED	Vulnerability - level 3	Vuln
351467	Amazon Linux Security Advisory for curl: ALAS2-2018-1135	Vulnerability - level 2	Vuln
351490	Amazon Linux Security Advisory for curl: ALAS-2019-1148	Vulnerability - level 2	Vuln
351506	Amazon Linux Security Advisory for curl: ALAS2-2019-1162	Vulnerability - level 3	Vuln
351523	Amazon Linux Security Advisory for curl: AL2012-2019-274	Vulnerability - level 2	Vuln
351565	Amazon Linux Security Advisory for python34: ALAS-2019-1202	Vulnerability - level 4	Vuln
351568	Amazon Linux Security Advisory for python3: ALAS2-2019-1204	Vulnerability - level 4	Vuln
351581	Amazon Linux Security Advisory for python36: ALAS-2019-1204	Vulnerability - level 4	Vuln
351601	Amazon Linux Security Advisory for python27: ALAS-2019-1230	Vulnerability - level 3	Vuln
351602	Amazon Linux Security Advisory for python: ALAS2-2019-1230	Vulnerability - level 4	Vuln
351625	Amazon Linux Security Advisory for python35: ALAS-2019-1243	Vulnerability - level 3	Vuln
351660	Amazon Linux Security Advisory for curl: ALAS-2016-742	Vulnerability - level 2	Vuln
351662	Amazon Linux Security Advisory for openssh: ALAS-2017-898	Vulnerability - level 3	Vuln

351699	Amazon Linux Security Advisory for nss: ALAS2-2019-1305	Vulnerability - level 3	Vuln
351710	Amazon Linux Security Advisory for python26: AL2012-2019-283	Vulnerability - level 4	Vuln
351750	Amazon Linux Security Advisory for subversion: ALAS-2019-1317	Vulnerability - level 4	Vuln
351780	Amazon Linux Security Advisory for python34: ALAS-2019-1324	Vulnerability - level 4	Vuln
351806	Amazon Linux Security Advisory for rssh: ALAS-2019-1328	Vulnerability - level 4	Vuln
351808	Amazon Linux Security Advisory for nss-softokn: ALAS2-2020-1379	Vulnerability - level 3	Vuln
351820	Amazon Linux Security Advisory for nss: ALAS2-2020-1384	Vulnerability - level 4	Vuln
351843	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS-2020-1344	Vulnerability - level 2	Vuln
351861	Amazon Linux Security Advisory for tomcat: ALAS2-2020-1402	Vulnerability - level 4	Vuln
351863	Amazon Linux Security Advisory for nss: ALAS-2020-1355	Vulnerability - level 4	Vuln
351869	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-2020-1406	Vulnerability - level 4	Vuln
351872	Amazon Linux Security Advisory for nss-softokn: AL2012-2020-300	Vulnerability - level 4	Vuln
351882	Amazon Linux Security Advisory for libvncserver: ALAS2-2020-1411	Vulnerability - level 4	Vuln
351943	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): AL2012-2020-305	Vulnerability - level 3	Vuln
351951	Amazon Linux Security Advisory for microcode_ctl: ALAS2-2020-1444	Vulnerability - level 3	Vuln
351952	Amazon Linux Security Advisory for nghttp2: ALAS2-2020-1445	Vulnerability - level 4	Vuln
351968	Amazon Linux Security Advisory for kernel: ALAS-2020-1401	Vulnerability - level 4	Vuln
351971	Amazon Linux Security Advisory for microcode_ctl: ALAS-2020-1396	Vulnerability - level 3	Vuln
351985	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL11): ALAS2-2020-1456	Vulnerability - level 3	Vuln
351995	Amazon Linux Security Advisory for kernel: ALAS2-2020-1465	Vulnerability - level 4	Vuln
352004	Amazon Linux Security Advisory for nghttp2: ALAS-2020-1404	Vulnerability - level 4	Vuln
352084	Amazon Linux Security Advisory for subversion: ALAS2-2020-1549	Vulnerability - level 3	Vuln
352092	Amazon Linux Security Advisory for libxml2: ALAS2-2020-1534	Vulnerability - level 3	Vuln
352122	Amazon Linux Security Advisory for ipa: ALAS2-2020-1519	Vulnerability - level 3	Vuln
352138	Amazon Linux Security Advisory for libxml2: ALAS-2020-1438	Vulnerability - level 3	Vuln
352169	Amazon Linux Security Advisory for kernel: ALAS2-2020-1566	Vulnerability - level 4	Vuln
352172	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-2020-1573	Vulnerability - level 4	Vuln
352175	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS-2020-1456	Vulnerability - level 4	Vuln
352181	Amazon Linux Security Advisory for libuv: ALAS2-2021-1581	Vulnerability - level 4	Vuln
352206	Amazon Linux Security Advisory for kernel: ALAS-2021-1461	Vulnerability - level 3	Vuln
352225	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-2021-1608	Vulnerability - level 3	Vuln
352237	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS-2021-1482	Vulnerability - level 3	Vuln
352243	Amazon Linux Security Advisory for bind: ALAS-2021-1485	Vulnerability - level 4	Vuln
352246	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL11): ALAS2-2021-1612	Vulnerability - level 3	Vuln
352252	Amazon Linux Security Advisory for bind: ALAS2-2021-1614	Vulnerability - level 4	Vuln
352258	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL11): ALAS2-2021-1622	Vulnerability - level 4	Vuln
352296	Amazon Linux Security Update for Open Secure Sockets Layer (OpenSSL): AL2012-2021-339	Vulnerability - level 3	Vuln
352300	Amazon Linux Security Advisory for kernel: ALAC2012-2020-020	Vulnerability - level 4	Vuln
352301	Amazon Linux Security Advisory for kernel: ALAC2012-2021-021	Vulnerability - level 4	Vuln
352302	Amazon Linux Security Advisory for kmod-sfc: ALAC2012-2021-022	Vulnerability - level 4	Vuln
352303	Amazon Linux Security Advisory for kmod-mlx5: ALAC2012-2021-023	Vulnerability - level 4	Vuln
352309	Amazon Linux Security Advisory for kernel: AMZN2KERNEL-INT-2020-004	Vulnerability - level 3	Vuln
352373	Amazon Linux Security Advisory for openldap: ALAS2-2021-1638	Vulnerability - level 3	Vuln

352376	Amazon Linux Security Advisory for bind: ALAS2-2021-1635	Vulnerability - level 4	Vuln
352392	Amazon Linux Security Advisory for libxml2: ALAS2-2021-1662	Vulnerability - level 3	Vuln
352395	Amazon Linux Security Advisory for httpd: ALAS2-2021-1659	Vulnerability - level 4	Vuln
352404	Amazon Linux Security Advisory for bind: ALAS2-2021-1651	Vulnerability - level 3	Vuln
352435	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-2021-1608-INT	Vulnerability - level 3	Vuln
352439	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL11): ALAS2-2021-1612-INT	Vulnerability - level 3	Vuln
352441	Amazon Linux Security Advisory for bind: ALAS2-2021-1614-INT	Vulnerability - level 4	Vuln
352447	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL11): ALAS2-2021-1622-INT	Vulnerability - level 4	Vuln
352451	Amazon Linux Security Advisory for libuv: ALAS2-2021-1581-INT	Vulnerability - level 4	Vuln
352459	Amazon Linux Security Advisory for libxml2: ALAS2-2021-1677	Vulnerability - level 3	Vuln
352462	Amazon Linux Security Advisory for httpd: ALAS2-2021-1674	Vulnerability - level 3	Vuln
352471	Amazon Linux Security Advisory for postgresql96: ALAS-2021-1520	Vulnerability - level 4	Vuln
352477	Amazon Linux Security Advisory for httpd24: ALAS-2021-1514	Vulnerability - level 3	Vuln
352483	Amazon Linux Security Advisory for bind: ALAS-2021-1508	Vulnerability - level 4	Vuln
352490	Amazon Linux Security Advisory for grub2: ALAS2-2021-1684	Vulnerability - level 3	Vuln
352506	Amazon Linux Security Advisory for curl: ALAS2-2021-1693	Vulnerability - level 3	Vuln
352831	Amazon Linux Security Advisory for kernel: ALAC2012-2021-030	Vulnerability - level 4	Vuln
352832	Amazon Linux Security Advisory for kmod-sfc: ALAC2012-2021-031	Vulnerability - level 4	Vuln
352833	Amazon Linux Security Advisory for kmod-mlx5: ALAC2012-2021-032	Vulnerability - level 4	Vuln
352846	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS-2021-1541	Vulnerability - level 3	Vuln
352847	Amazon Linux Security Advisory for containerd: ALAS-2021-1540	Vulnerability - level 3	Vuln
352848	Amazon Linux Security Advisory for golang: ALAS-2021-1538	Vulnerability - level 3	Vuln
352849	Amazon Linux Security Advisory for docker: ALAS-2021-1537	Vulnerability - level 3	Vuln
352853	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL)11: ALAS2-2021-1714	Vulnerability - level 3	Vuln
352857	Amazon Linux Security Advisory for httpd24: ALAS-2021-1543	Vulnerability - level 4	Vuln
352858	Amazon Linux Security Advisory for httpd: ALAS2-2021-1716	Vulnerability - level 4	Vuln
352867	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-2021-1721	Vulnerability - level 3	Vuln
352869	Amazon Linux Security Advisory for kernel: ALAS2-2021-1719	Vulnerability - level 4	Vuln
352872	Amazon Linux Security Advisory for java-11-amazon-corretto : ALAS2-2021-1718	Vulnerability - level 4	Vuln
353093	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : AL2012-2021-354	Vulnerability - level 3	Vuln
353094	Amazon Linux Security Advisory for golang : AL2012-2021-355	Vulnerability - level 3	Vuln
353100	Amazon Linux Security Advisory for kernel : ALAC2012-2021-024	Vulnerability - level 4	Vuln
353101	Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025	Vulnerability - level 4	Vuln
353102	Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026	Vulnerability - level 4	Vuln
353116	Amazon Linux Security Advisory for busybox : ALAS-2022-1558	Vulnerability - level 4	Vuln
353139	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-012	Vulnerability - level 4	Vuln
353147	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-004	Vulnerability - level 4	Vuln
353158	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-002	Vulnerability - level 4	Vuln
353176	Amazon Linux Security Advisory for expat : ALAS-2022-1569	Vulnerability - level 5	Vuln
353182	Amazon Linux Security Advisory for expat : ALAS2-2022-1754	Vulnerability - level 5	Vuln
353184	Amazon Linux Security Advisory for kernel : ALAS-2022-1571	Vulnerability - level 4	Vuln
353186	Amazon Linux Security Advisory for docker : ALAS2NITRO-ENCLAVES-2022-017	Vulnerability - level 4	Vuln
353187	Amazon Linux Security Advisory for containerd : ALAS2NITRO-ENCLAVES-2022-016	Vulnerability - level 4	Vuln

353189	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-023	Vulnerability - level 3	Vuln
353190	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-011	Vulnerability - level 3	Vuln
353191	Amazon Linux Security Advisory for docker : ALAS2DOCKER-2022-017	Vulnerability - level 4	Vuln
353192	Amazon Linux Security Advisory for containerd : ALAS2DOCKER-2022-016	Vulnerability - level 4	Vuln
353195	Amazon Linux Security Advisory for kernel : ALAS2-2022-1761	Vulnerability - level 4	Vuln
353198	Amazon Linux Security Advisory for expat : ALAS-2022-1573	Vulnerability - level 5	Vuln
353200	Amazon Linux Security Advisory for expat : ALAS2-2022-1764	Vulnerability - level 5	Vuln
353210	Amazon Linux Security Advisory for openldap : ALAS2-2022-1770	Vulnerability - level 4	Vuln
353215	Amazon Linux Security Advisory for kernel : ALAS-2022-1581	Vulnerability - level 4	Vuln
353216	Amazon Linux Security Advisory for kernel : ALAS2-2022-1774	Vulnerability - level 4	Vuln
353237	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-025	Vulnerability - level 4	Vuln
353238	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-013	Vulnerability - level 4	Vuln
353241	Amazon Linux Security Advisory for busybox : AL2012-2022-358	Vulnerability - level 4	Vuln
353242	Amazon Linux Security Advisory for kernel : ALAC2012-2022-036	Vulnerability - level 4	Vuln
353243	Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2022-037	Vulnerability - level 4	Vuln
353244	Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2022-038	Vulnerability - level 4	Vuln
353262	Amazon Linux Security Advisory for thunderbird : ALAS2-2022-1779	Vulnerability - level 5	Vuln
353263	Amazon Linux Security Advisory for golang : ALAS2-2022-1776	Vulnerability - level 5	Vuln
353269	Amazon Linux Security Advisory for httpd : ALAS2-2022-1783	Vulnerability - level 5	Vuln
353274	Amazon Linux Security Advisory for httpd24 : ALAS-2022-1584	Vulnerability - level 5	Vuln
353275	Amazon Linux Security Advisory for golang : ALAS-2022-1583	Vulnerability - level 5	Vuln
353283	Amazon Linux Security Advisory for expat: ALAS2-INT-2022-1754	Vulnerability - level 5	Vuln
353289	Amazon Linux Security Advisory for expat: ALAS2-INT-2022-1764	Vulnerability - level 5	Vuln
353293	Amazon Linux Security Advisory for kernel : ALAS2-2022-1793	Vulnerability - level 4	Vuln
353305	Amazon Linux Security Advisory for ntp: ALAS2-INT-2018-1009	Vulnerability - level 4	Vuln
353328	Amazon Linux Security Advisory for openssh: ALAS2-INT-2018-1042	Vulnerability - level 3	Vuln
353335	Amazon Linux Security Advisory for kernel: ALAS2-INT-2018-1050	Vulnerability - level 4	Vuln
353360	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2-INT-2018-1102	Vulnerability - level 4	Vuln
353367	Amazon Linux Security Advisory for wpa_supplicant: ALAS2-INT-2018-1122	Vulnerability - level 3	Vuln
353369	Amazon Linux Security Advisory for xerces-c: ALAS2-INT-2018-1124	Vulnerability - level 4	Vuln
353378	Amazon Linux Security Advisory for curl: ALAS2-INT-2018-1135	Vulnerability - level 5	Vuln
353430	Amazon Linux Security Advisory for python3: ALAS2-INT-2019-1204	Vulnerability - level 5	Vuln
353446	Amazon Linux Security Advisory for python: ALAS2-INT-2019-1230	Vulnerability - level 5	Vuln
353481	Amazon Linux Security Advisory for nss: ALAS2-INT-2019-1305	Vulnerability - level 3	Vuln
353542	Amazon Linux Security Advisory for nss-softokn: ALAS2-INT-2020-1379	Vulnerability - level 4	Vuln
353546	Amazon Linux Security Advisory for nss: ALAS2-INT-2020-1384	Vulnerability - level 4	Vuln
353562	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-INT-2020-1406	Vulnerability - level 2	Vuln
353566	Amazon Linux Security Advisory for libvncserver: ALAS2-INT-2020-1411	Vulnerability - level 4	Vuln
353593	Amazon Linux Security Advisory for microcode_ctl: ALAS2-INT-2020-1444	Vulnerability - level 3	Vuln
353594	Amazon Linux Security Advisory for nghttp2: ALAS2-INT-2020-1445	Vulnerability - level 4	Vuln

353605	Amazon Linux Security Advisory for Open Secure Sockets Layer11 (OpenSSL11): ALAS2-INT-2020-1456	Vulnerability - level 3	Vuln
353659	Amazon Linux Security Advisory for ipa: ALAS2-INT-2020-1519	Vulnerability - level 3	Vuln
353673	Amazon Linux Security Advisory for libxml2: ALAS2-INT-2020-1534	Vulnerability - level 4	Vuln
353687	Amazon Linux Security Advisory for subversion: ALAS2-INT-2020-1549	Vulnerability - level 3	Vuln
353707	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) openssl11: ALAS2-INT-2020-1573	Vulnerability - level 3	Vuln
353737	Amazon Linux Security Advisory for openssl11: ALAS2-INT-2021-1612	Vulnerability - level 4	Vuln
353739	Amazon Linux Security Advisory for bind: ALAS2-INT-2021-1614	Vulnerability - level 4	Vuln
353746	Amazon Linux Security Advisory for openssl11: ALAS2-INT-2021-1622	Vulnerability - level 4	Vuln
353755	Amazon Linux Security Advisory for bind: ALAS2-INT-2021-1635	Vulnerability - level 4	Vuln
353758	Amazon Linux Security Advisory for openldap: ALAS2-INT-2021-1638	Vulnerability - level 4	Vuln
353769	Amazon Linux Security Advisory for bind: ALAS2-INT-2021-1651	Vulnerability - level 3	Vuln
353779	Amazon Linux Security Advisory for libxml2: ALAS2-INT-2021-1662	Vulnerability - level 4	Vuln
353791	Amazon Linux Security Advisory for httpd: ALAS2-INT-2021-1674	Vulnerability - level 5	Vuln
353794	Amazon Linux Security Advisory for libxml2: ALAS2-INT-2021-1677	Vulnerability - level 4	Vuln
353807	Amazon Linux Security Advisory for curl: ALAS2-INT-2021-1693	Vulnerability - level 4	Vuln
353825	Amazon Linux Security Advisory for Open Secure Sockets Layer11 (OpenSSL11): ALAS2-INT-2021-1714	Vulnerability - level 4	Vuln
353827	Amazon Linux Security Advisory for httpd: ALAS2-INT-2021-1716	Vulnerability - level 5	Vuln
353829	Amazon Linux Security Advisory for kernel: ALAS2-INT-2021-1719	Vulnerability - level 4	Vuln
353831	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-INT-2021-1721	Vulnerability - level 4	Vuln
353843	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-INT-2018-1004	Vulnerability - level 3	Vuln
353850	Amazon Linux Security Advisory for curl: ALAS2-INT-2019-1162	Vulnerability - level 5	Vuln
353865	Amazon Linux Security Advisory for tomcat: ALAS2-INT-2020-1402	Vulnerability - level 5	Vuln
353878	Amazon Linux Security Advisory for kernel: ALAS2-INT-2020-1566	Vulnerability - level 4	Vuln
353882	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-INT-2021-1608	Vulnerability - level 4	Vuln
353885	Amazon Linux Security Advisory for grub2: ALAS2-INT-2021-1684	Vulnerability - level 4	Vuln
353888	Amazon Linux Security Advisory for java-11-amazon-corretto: ALAS2-INT-2021-1718	Vulnerability - level 4	Vuln
353894	Amazon Linux Security Advisory for kernel: ALAS2-INT-2022-1761	Vulnerability - level 4	Vuln
353906	Amazon Linux Security Advisory for libuv: ALAS2-INT-2021-1581	Vulnerability - level 4	Vuln
353936	Amazon Linux Security Advisory for kernel: AMZN2KERNEL-INT-2022-028	Vulnerability - level 4	Vuln
353937	Amazon Linux Security Advisory for xmlrpc-c : ALAS-2022-1585	Vulnerability - level 5	Vuln
353940	Amazon Linux Security Advisory for xmlrpc-c : ALAS2-2022-1795	Vulnerability - level 5	Vuln
353941	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2-2022-1801	Vulnerability - level 5	Vuln
353947	Amazon Linux Security Advisory for kernel : ALAS2-2022-1798	Vulnerability - level 4	Vuln
353956	Amazon Linux Security Advisory for kernel : ALAS-2022-1591	Vulnerability - level 4	Vuln
353960	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-014	Vulnerability - level 4	Vuln
353962	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-026	Vulnerability - level 4	Vuln
353964	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-001	Vulnerability - level 4	Vuln
353970	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS-2022-1605	Vulnerability - level 5	Vuln
353971	Amazon Linux Security Advisory for httpd24 : ALAS-2022-1607	Vulnerability - level 5	Vuln
353975	Amazon Linux Security Advisory for expat : ALAS-2022-1603	Vulnerability - level 5	Vuln
353976	Amazon Linux Security Advisory for kernel : ALAS-2022-1604	Vulnerability - level 4	Vuln
353977	Amazon Linux Security Advisory for golang : ALAS2-2022-1811	Vulnerability - level 5	Vuln

353983	Amazon Linux Security Advisory for openssl11 : ALAS2-2022-1815	Vulnerability - level 5	Vuln
353985	Amazon Linux Security Advisory for kernel : ALAS2-2022-1813	Vulnerability - level 4	Vuln
353986	Amazon Linux Security Advisory for expat : ALAS2-2022-1809	Vulnerability - level 5	Vuln
353987	Amazon Linux Security Advisory for amazon-ssm-agent : ALAS2-2022-1807	Vulnerability - level 4	Vuln
353988	Amazon Linux Security Advisory for httpd : ALAS2-2022-1812	Vulnerability - level 5	Vuln
353993	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-016	Vulnerability - level 4	Vuln
353994	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-028	Vulnerability - level 4	Vuln
354006	Amazon Linux Security Advisory for libxml2 : ALAS2-2022-1826	Vulnerability - level 4	Vuln
354007	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-015	Vulnerability - level 4	Vuln
354008	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-030	Vulnerability - level 4	Vuln
354017	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-032	Vulnerability - level 4	Vuln
354023	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-017	Vulnerability - level 4	Vuln
354035	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS-2022-1626	Vulnerability - level 5	Vuln
354040	Amazon Linux Security Advisory for Open Secure Sockets Layer11 (OpenSSL11) : ALAS2-2022-1832	Vulnerability - level 5	Vuln
354041	Amazon Linux Security Advisory for golang : ALAS2-2022-1830	Vulnerability - level 5	Vuln
354042	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2-2022-1831	Vulnerability - level 5	Vuln
354044	Amazon Linux Security Advisory for kernel : ALAS2-2022-1833	Vulnerability - level 4	Vuln
354049	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-034	Vulnerability - level 4	Vuln
354051	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-019	Vulnerability - level 4	Vuln
354055	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-007	Vulnerability - level 4	Vuln
354064	Amazon Linux Security Advisory for golist : ALAS2-2022-1847	Vulnerability - level 5	Vuln
354067	Amazon Linux Security Advisory for golang : ALAS2-2022-1846	Vulnerability - level 5	Vuln
354069	Amazon Linux Security Advisory for golang : ALAS-2022-1635	Vulnerability - level 5	Vuln
354071	Amazon Linux Security Advisory for kernel : ALAS-2022-1636	Vulnerability - level 4	Vuln
354075	Amazon Linux Security Advisory for kernel : ALAS2-2022-1852	Vulnerability - level 4	Vuln
354083	Amazon Linux Security Advisory for runc : ALAS2DOCKER-2022-020	Vulnerability - level 5	Vuln
354088	Amazon Linux Security Advisory for golang-github-syndtr-gocapability : ALAS2-2022-1865	Vulnerability - level 5	Vuln
354089	Amazon Linux Security Advisory for golang-googlecode-sqlite : ALAS2-2022-1862	Vulnerability - level 5	Vuln
354090	Amazon Linux Security Advisory for golang-github-kr-pty : ALAS2-2022-1864	Vulnerability - level 5	Vuln
354091	Amazon Linux Security Advisory for go-rpm-macros : ALAS2-2022-1863	Vulnerability - level 5	Vuln
354092	Amazon Linux Security Advisory for golang-googlecode-net : ALAS2-2022-1861	Vulnerability - level 5	Vuln
354093	Amazon Linux Security Advisory for golang-github-gorilla-mux : ALAS2-2022-1860	Vulnerability - level 5	Vuln
354094	Amazon Linux Security Advisory for golang-github-gorilla-context : ALAS2-2022-1859	Vulnerability - level 5	Vuln
354096	Amazon Linux Security Advisory for golang-github-godbus-dbus : ALAS2-2022-1858	Vulnerability - level 5	Vuln
354124	Amazon Linux Security Advisory for e2fsprogs : ALAS2-2022-1884	Vulnerability - level 4	Vuln
354144	Amazon Linux Security Advisory for openldap: ALAS2-INT-2022-1770	Vulnerability - level 4	Vuln

354148	Amazon Linux Security Advisory for kernel: ALAS2-INT-2022-1774	Vulnerability - level 4	Vuln
354149	Amazon Linux Security Advisory for golang: ALAS2-INT-2022-1776	Vulnerability - level 5	Vuln
354151	Amazon Linux Security Advisory for thunderbird: ALAS2-INT-2022-1779	Vulnerability - level 5	Vuln
354154	Amazon Linux Security Advisory for httpd: ALAS2-INT-2022-1783	Vulnerability - level 5	Vuln
354163	Amazon Linux Security Advisory for kernel: ALAS2-INT-2022-1793	Vulnerability - level 4	Vuln
354165	Amazon Linux Security Advisory for xmlrpc-c: ALAS2-INT-2022-1795	Vulnerability - level 5	Vuln
354167	Amazon Linux Security Advisory for kernel: ALAS2-INT-2022-1798	Vulnerability - level 4	Vuln
354170	Amazon Linux Security Advisory for openssl: ALAS2-INT-2022-1801	Vulnerability - level 5	Vuln
354176	Amazon Linux Security Advisory for amazon-ssm-agent: ALAS2-INT-2022-1807	Vulnerability - level 4	Vuln
354178	Amazon Linux Security Advisory for expat: ALAS2-INT-2022-1809	Vulnerability - level 5	Vuln
354180	Amazon Linux Security Advisory for golang: ALAS2-INT-2022-1811	Vulnerability - level 5	Vuln
354181	Amazon Linux Security Advisory for httpd: ALAS2-INT-2022-1812	Vulnerability - level 5	Vuln
354183	Amazon Linux Security Advisory for openssl11: ALAS2-INT-2022-1815	Vulnerability - level 5	Vuln
354193	Amazon Linux Security Advisory for libxml2: ALAS2-INT-2022-1826	Vulnerability - level 4	Vuln
354197	Amazon Linux Security Advisory for golang: ALAS2-INT-2022-1830	Vulnerability - level 5	Vuln
354198	Amazon Linux Security Advisory for openssl: ALAS2-INT-2022-1831	Vulnerability - level 5	Vuln
354199	Amazon Linux Security Advisory for openssl11: ALAS2-INT-2022-1832	Vulnerability - level 5	Vuln
354208	Amazon Linux Security Advisory for golang: ALAS2-INT-2022-1846	Vulnerability - level 5	Vuln
354209	Amazon Linux Security Advisory for golist: ALAS2-INT-2022-1847	Vulnerability - level 5	Vuln
354218	Amazon Linux Security Advisory for golang-github-godbus-dbus: ALAS2-INT-2022-1858	Vulnerability - level 5	Vuln
354219	Amazon Linux Security Advisory for golang-github-gorilla-context: ALAS2-INT-2022-1859	Vulnerability - level 5	Vuln
354220	Amazon Linux Security Advisory for golang-github-gorilla-mux: ALAS2-INT-2022-1860	Vulnerability - level 5	Vuln
354221	Amazon Linux Security Advisory for golang-googlecode-net: ALAS2-INT-2022-1861	Vulnerability - level 5	Vuln
354222	Amazon Linux Security Advisory for golang-googlecode-sqlite: ALAS2-INT-2022-1862	Vulnerability - level 5	Vuln
354223	Amazon Linux Security Advisory for go-rpm-macros: ALAS2-INT-2022-1863	Vulnerability - level 5	Vuln
354224	Amazon Linux Security Advisory for golang-github-kr-pty: ALAS2-INT-2022-1864	Vulnerability - level 5	Vuln
354225	Amazon Linux Security Advisory for golang-github-syndtr-gocapability: ALAS2-INT-2022-1865	Vulnerability - level 5	Vuln
354229	Amazon Linux Security Advisory for kernel: AMZN2KERNEL-INT-2022-029	Vulnerability - level 4	Vuln
354230	Amazon Linux Security Advisory for kernel: AMZN2KERNEL-INT-2022-030	Vulnerability - level 4	Vuln
354231	Amazon Linux Security Advisory for kernel: AMZN2KERNEL-INT-2022-031	Vulnerability - level 4	Vuln
354232	Amazon Linux Security Advisory for kernel: AMZN2KERNEL-INT-2022-032	Vulnerability - level 4	Vuln
354233	Amazon Linux Security Advisory for kernel: AMZN2KERNEL-INT-2022-034	Vulnerability - level 4	Vuln
354241	Amazon Linux Security Advisory for kernel: ALAS2-INT-2022-1813	Vulnerability - level 4	Vuln
354242	Amazon Linux Security Advisory for kernel: ALAS2-INT-2022-1833	Vulnerability - level 4	Vuln
354244	Amazon Linux Security Advisory for kernel: ALAS2-INT-2022-1852	Vulnerability - level 4	Vuln
354279	Amazon Linux Security Advisory for kernel : ALAS2022-2022-039	Vulnerability - level 4	Vuln
354286	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2022-2022-147	Vulnerability - level 3	Vuln
354299	Amazon Linux Security Advisory for xmlrpc-c : ALAS2022-2022-080	Vulnerability - level 5	Vuln

354327	Amazon Linux Security Advisory for kernel : ALAS2022-2022-083	Vulnerability - level 4	Vuln
354355	Amazon Linux Security Advisory for Open Secure Sockets Layer1.1 (OpenSSL1.1) : ALAS2022-2022-105	Vulnerability - level 5	Vuln
354360	Amazon Linux Security Advisory for expat : ALAS2022-2022-017	Vulnerability - level 5	Vuln
354370	Amazon Linux Security Advisory for golang-github-cpuguy83-md2man : ALAS2022-2022-140	Vulnerability - level 5	Vuln
354371	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2022-2022-123	Vulnerability - level 5	Vuln
354380	Amazon Linux Security Advisory for e2fsprogs : ALAS2022-2022-228	Vulnerability - level 4	Vuln
354384	Amazon Linux Security Advisory for bind : ALAS2022-2022-166	Vulnerability - level 3	Vuln
354401	Amazon Linux Security Advisory for golang : ALAS2022-2021-007	Vulnerability - level 5	Vuln
354410	Amazon Linux Security Advisory for bind : ALAS2022-2022-138	Vulnerability - level 3	Vuln
354427	Amazon Linux Security Advisory for expat : ALAS2022-2022-028	Vulnerability - level 5	Vuln
354434	Amazon Linux Security Advisory for expat : ALAS2022-2022-232	Vulnerability - level 5	Vuln
354439	Amazon Linux Security Advisory for kernel : ALAS2022-2022-150	Vulnerability - level 4	Vuln
354459	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2022-2022-195	Vulnerability - level 5	Vuln
354464	Amazon Linux Security Advisory for libxml2 : ALAS2022-2022-198	Vulnerability - level 4	Vuln
354468	Amazon Linux Security Advisory for kernel : ALAS2022-2022-185	Vulnerability - level 4	Vuln
354481	Amazon Linux Security Advisory for httpd : ALAS2022-2022-053	Vulnerability - level 5	Vuln
354482	Amazon Linux Security Advisory for httpd : ALAS2022-2022-202	Vulnerability - level 5	Vuln
354486	Amazon Linux Security Advisory for libxml2 : ALAS2022-2022-068	Vulnerability - level 4	Vuln
354488	Amazon Linux Security Advisory for golang : ALAS2022-2022-009	Vulnerability - level 4	Vuln
354490	Amazon Linux Security Advisory for expat : ALAS2022-2022-036	Vulnerability - level 5	Vuln
354493	Amazon Linux Security Advisory for golist : ALAS2022-2022-133	Vulnerability - level 5	Vuln
354499	Amazon Linux Security Advisory for kernel : ALAS2022-2022-042	Vulnerability - level 4	Vuln
354504	Amazon Linux Security Advisory for golist : ALAS2022-2022-192	Vulnerability - level 5	Vuln
354511	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2022-2022-104	Vulnerability - level 5	Vuln
354513	Amazon Linux Security Advisory for httpd : ALAS2022-2022-110	Vulnerability - level 5	Vuln
354527	Amazon Linux Security Advisory for golang : ALAS2022-2022-193	Vulnerability - level 5	Vuln
354606	Amazon Linux Security Advisory for e2fsprogs: ALAS2-INT-2022-1884	Vulnerability - level 4	Vuln
354627	Amazon Linux Security Advisory for expat : AL2012-2022-359	Vulnerability - level 5	Vuln
354629	Amazon Linux Security Advisory for xmlrpc-c : AL2012-2022-361	Vulnerability - level 5	Vuln
354636	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : AL2012-2022-368	Vulnerability - level 5	Vuln
354638	Amazon Linux Security Advisory for libxml2 : AL2012-2022-370	Vulnerability - level 4	Vuln
354639	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : AL2012-2022-371	Vulnerability - level 5	Vuln
354653	Amazon Linux Security Advisory for pcs : ALAS2-2023-1905	Vulnerability - level 3	Vuln
354734	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS-2023-1683	Vulnerability - level 4	Vuln
354735	Amazon Linux Security Advisory for Open Secure Sockets Layer11 (OpenSSL11) : ALAS2-2023-1934	Vulnerability - level 4	Vuln
354737	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2-2023-1935	Vulnerability - level 4	Vuln
354771	Amazon Linux Security Advisory for nss-util : ALAS2-2023-1942	Vulnerability - level 4	Vuln
354802	Amazon Linux Security Advisory for openssl11 : ALAS2-2023-1974	Vulnerability - level 3	Vuln
354835	Amazon Linux Security Advisory for bind : ALAS2-2023-2001	Vulnerability - level 4	Vuln
354864	Amazon Linux Security Advisory for Open Virtual Private Network (OpenVPN) : ALAS-2023-1719	Vulnerability - level 5	Vuln
354907	Amazon Linux Security Advisory for openldap : ALAS2-2023-2033	Vulnerability - level 4	Vuln
354925	Amazon Linux Security Advisory for openldap : ALAS-2023-1741	Vulnerability - level 4	Vuln
354929	Amazon Linux Security Advisory for libxml2 : ALAS-2023-1743	Vulnerability - level 5	Vuln
354933	Amazon Linux Security Advisory for pcs: ALAS2-INT-2023-1905	Vulnerability - level 3	Vuln
354960	Amazon Linux Security Advisory for openssl11: ALAS2-INT-2023-1934	Vulnerability - level 4	Vuln

354961	Amazon Linux Security Advisory for openssl: ALAS2-INT-2023-1935	Vulnerability - level 4	Vuln
354987	Amazon Linux Security Advisory for openssl11: ALAS2-INT-2023-1974	Vulnerability - level 3	Vuln
355013	Amazon Linux Security Advisory for bind: ALAS2-INT-2023-2001	Vulnerability - level 4	Vuln
355045	Amazon Linux Security Advisory for openldap: ALAS2-INT-2023-2033	Vulnerability - level 4	Vuln
355058	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : AL2012-2023-382	Vulnerability - level 4	Vuln
355075	Amazon Linux Security Advisory for Open Virtual Private Network (OpenVPN) : AL2012-2023-399	Vulnerability - level 5	Vuln
355082	Amazon Linux Security Advisory for openldap : AL2012-2023-407	Vulnerability - level 4	Vuln
355111	Amazon Linux Security Advisory for golist : ALAS2023-2023-046	Vulnerability - level 4	Vuln
355133	Amazon Linux Security Advisory for e2fsprogs : ALAS2023-2023-044	Vulnerability - level 4	Vuln
355147	Amazon Linux Security Advisory for bind : ALAS2023-2023-010	Vulnerability - level 3	Vuln
355186	Amazon Linux Security Advisory for golang-github-cpuguy83-md2man : ALAS2023-2023-047	Vulnerability - level 4	Vuln
355199	Amazon Linux Security Advisory for kernel : ALAS2023-2023-070	Vulnerability - level 4	Vuln
355200	Amazon Linux Security Advisory for xmlrpc-c : ALAS2023-2023-068	Vulnerability - level 5	Vuln
355209	Amazon Linux Security Advisory for libxml2 : ALAS2023-2023-096	Vulnerability - level 4	Vuln
355212	Amazon Linux Security Advisory for golang : ALAS2023-2023-048	Vulnerability - level 5	Vuln
355230	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-101	Vulnerability - level 4	Vuln
355250	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-051	Vulnerability - level 5	Vuln
355252	Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-054	Vulnerability - level 4	Vuln
355264	Amazon Linux Security Advisory for httpd : ALAS2023-2023-072	Vulnerability - level 5	Vuln
355273	Amazon Linux Security Advisory for nodejs : ALAS2023-2023-084	Vulnerability - level 5	Vuln
355281	Amazon Linux Security Advisory for expat : ALAS2023-2023-058	Vulnerability - level 5	Vuln
355404	Amazon Linux Security Advisory for libldb : ALAS2023-2023-187	Vulnerability - level 3	Vuln
355410	Amazon Linux Security Advisory for samba : ALAS2023-2023-190	Vulnerability - level 3	Vuln
355418	Amazon Linux Security Advisory for samba : ALAS2023-2023-206	Vulnerability - level 3	Vuln
370008	Apple Safari 9.1.1 Not Installed (APPLE-SA-2016-05-16-5)	Vulnerability - level 4	Vuln
370017	NTP Multiple Security Vulnerabilities	Vulnerability - level 3	Practice
370021	Citrix XenServer Security Update (CTX212736)	Vulnerability - level 4	Vuln
370041	Citrix XenServer Security Update (CTX140038)	Vulnerability - level 2	Vuln
370062	Adobe Brackets Multiple Vulnerabilities (APSB16-20)	Vulnerability - level 3	Vuln
370069	OpenSSL Multiple Security Advisories (secadv_20160503)	Vulnerability - level 4	Practice
370071	HP Data Protector Multiple Security Vulnerabilities (HPSBGN03580)	Vulnerability - level 4	Practice
370072	Unitronics VisiLogic OPLC IDE vlp File Parsing Stack Buffer Overflow Vulnerability	Vulnerability - level 3	Vuln
370077	Trihedral VTScada Multiple Vulnerabilities	Vulnerability - level 4	Vuln
370083	Adobe Flash Player Remote Code Execution Vulnerability (APSB16-25)	Vulnerability - level 5	Vuln
370085	Advantech WebAccess ActiveX Vulnerabilities	Vulnerability - level 3	Vuln
370095	Apple Mac OS X v10.11.6 and Security Update 2016-004 Not Installed (APPLE-SA-2016-07-18-1)	Vulnerability - level 5	Vuln
370183	HP Systems Insight Manager Multiple Vulnerabilities	Vulnerability - level 5	Vuln
370189	Red Hat Struts ActionForm Instance Remote Code Execution Vulnerability	Vulnerability - level 4	Vuln
370192	Apple Mac OS X v10.11 Not Installed (APPLE-SA-2015-09-30-3)	Vulnerability - level 4	Vuln
370198	cURL Multiple Security Vulnerabilities	Potential Vulnerability - level 3	Practice
370216	Apple Xcode v7.0 Not Installed (APPLE-SA-2015-09-16-2)	Vulnerability - level 4	Vuln
370229	Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilites (CPUJUL2015)	Vulnerability - level 3	Vuln

370230	Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUOCT2015)	Vulnerability - level 3	Vuln
370235	Moxa SoftCMS Multiple Vulnerabilities	Vulnerability - level 3	Vuln
370240	Moxa SoftCMS SQL Injection Vulnerability	Vulnerability - level 3	Vuln
370241	Moxa SoftCMS Multiple Buffer Overflow Vulnerabilities	Vulnerability - level 3	Vuln
370262	Apple macOS Sierra Security Update 10.12.2 Not Installed (APPLE-SA-2016-12-13-1)	Vulnerability - level 5	Vuln
370269	Arista EOS and CloudVision eXchange Multiple OpenSSL Vulnerabilities (Security Advisory 0024)	Potential Vulnerability - level 3	Practice
370284	HP SiteScope Remote Disclosure of Information Vulnerability (HPSBGN03694)	Vulnerability - level 3	Vuln
370304	Citrix License Server 11.14.0.1 or before HTTP Open Redirect Vulnerability (CTX220379)	Vulnerability - level 3	Vuln
370343	Ecava Integraxor Web Server SQL Injection Vulnerability	Vulnerability - level 3	Vuln
370348	Apple Mac OS X Security Update Sierra 10.12.4, El Capitan 2017-001 and Yosemite 2017-001 Not Installed (APPLE-SA-2017-03-27-3)	Vulnerability - level 4	Vuln
370355	Panasonic FPWIN Pro Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
370369	Microsoft Visual Studio for Mac Security Update April 2017	Vulnerability - level 4	Vuln
370373	IBM Notes Multiple Apache Struts Vulnerabilities (swg21988182)	Vulnerability - level 4	Vuln
370408	Schneider Electric Wonderware InduSoft Web Studio Local Privilege Escalation Vulnerability	Vulnerability - level 3	Vuln
370409	PACTware Denial of Service Vulnerability	Vulnerability - level 3	Vuln
370449	Ecava Integraxor SQL Injection Vulnerability	Vulnerability - level 3	Vuln
370450	Microsoft Skype Stack Buffer Overflow Vulnerability	Vulnerability - level 3	Vuln
370459	FlexNet Publisher Privilege Escalation Vulnerability (SA76368)	Vulnerability - level 4	Vuln
370467	GE Communicator Heap-Based Buffer Overflow Vulnerability.	Vulnerability - level 4	Vuln
370469	Oracle Java SE Critical Patch Update - July 2017	Vulnerability - level 5	Vuln
370475	Apple macOS Sierra Security Update 10.12.6, El Capitan 2017-003 and Yosemite 2017-003 Not Installed (2017-003)	Vulnerability - level 5	Vuln
370496	Tableau Server and Desktop Multiple Vulnerabilities (Important-ADV-2017-012)	Vulnerability - level 4	Vuln
370524	Elasticsearch Logstash Man in the Middle Security Bypass Vulnerability (ESA-2015-09)	Vulnerability - level 3	Vuln
370526	Elasticsearch Logstash Remote Command Execution Vulnerability (ESA-2014-02)	Vulnerability - level 4	Vuln
370527	McAfee Network Security Manager PHP HTTP redirect Vulnerability	Vulnerability - level 3	Vuln
370569	Apple Safari 11 Not Installed	Vulnerability - level 4	Vuln
370571	IBM WebSphere Application Server Java SDK Multiple Vulnerabilities (swg22007002)	Vulnerability - level 4	Practice
370577	Apple iTunes for Windows Prior to 12.7 Multiple Vulnerabilities. (HT208141)	Vulnerability - level 4	Vuln
370585	Apple iCloud for Windows Multiple Security Vulnerabilities (HT208142)	Vulnerability - level 5	Vuln
370599	Tableau Server and Desktop Elevation of privilege Vulnerability (Important-ADV-2017-017)	Vulnerability - level 3	Vuln
370601	Apache Cassandra Remote Code Execution Vulnerability (Unix Authenticated Check)	Vulnerability - level 3	Vuln
370625	Apple macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan Not Installed	Vulnerability - level 4	Vuln
370636	Multiple vulnerabilities in IBM Java SDK affect IBM Tivoli Monitoring	Vulnerability - level 4	Vuln
370649	Trihedral VTScada Multiple Vulnerabilities Prior to 11.3.05	Vulnerability - level 4	Vuln
370677	Apple macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan Not Installed	Vulnerability - level 4	Vuln
370710	Apple macOS Security Update for High Sierra Not Installed (Meltdown)	Vulnerability - level 4	Vuln
370729	Moxa MXview service path escalation Unquoted Vulnerability	Vulnerability - level 3	Vuln

370732	Schneider Electric Pelco VideoXpert Enterprise Multiple Vulnerabilities	Vulnerability - level 3	Vuln
370738	Apple macOS High Sierra 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan Not Installed (Meltdown)	Vulnerability - level 4	Vuln
370750	IBM WebSphere Application Server Vulnerabilities in Apache Struts(swg21985995)	Vulnerability - level 3	Practice
370755	IBM Java SDK Multiple Vulnerabilities (Oracle July 18 2017 CPU (1.6.0_161, 1.7.0_151, 1.8.0_141))	Vulnerability - level 4	Vuln
370758	IBM WebSphere Application Server XML External Entity Injection (XXE) Vulnerability (swg21978495)	Vulnerability - level 3	Practice
370760	Infineon Trusted Platform Module (TPM) Chipsets Mishandles RSA key Generation Vulnerability (ROCA)	Vulnerability - level 3	Vuln
370781	3S-Smart CODESYS GmbH Web Server Stack Based Buffer Overflow Vulnerability (ICSA-18-032-02)	Vulnerability - level 5	Vuln
370851	Apple macOS High Sierra 10.13.4, Security Update 2018-002 Sierra, and Security Update 2018-002 El Capitan Not Installed	Vulnerability - level 5	Vuln
370907	Wibu-Systems CodeMeter Runtime Privilege Escalation Vulnerability.	Vulnerability - level 4	Vuln
370911	InduSoft Web Studio and InTouch Machine Edition Remote Code Execution Vulnerability	Potential Vulnerability - level 4	Practice
370912	Multiple vulnerabilities affect the GSKit component of IBM Tivoli Monitoring versions 6.2.3 through 6.2.3 FP5 (swg22015424)	Vulnerability - level 4	Vuln
370915	Java JMX Server Insecure Configuration Remote Code Execution Vulnerability	Vulnerability - level 5	Vuln
370929	Delta PMSOFT Multiple stack-based buffer overflow vulnerability	Vulnerability - level 3	Vuln
370933	Delta Electronics WPLSOFT and PMSOFT Vulnerabilities	Vulnerability - level 3	Vuln
371014	IBM InfoSphere Information Server Multiple Vulnerabilities (swg22015468)	Vulnerability - level 4	Vuln
371033	F5 BIG-IP ASM TLS vulnerability (K16674)	Vulnerability - level 3	Vuln
371045	F5 BIG-IP ASM Multiple Vulnerabilities (K24578092,K29146534,K51801290,K93472064)	Vulnerability - level 4	Vuln
371063	Java JMX Server Insecure Configuration Vulnerability (DEPRECATED)	Vulnerability - level 5	Vuln
371100	F5 BIG-IP Application Security Manager (ASM) Open Secure Sockets Layer (OpenSSL) Vulnerability (K59298921)	Vulnerability - level 3	Vuln
371118	IBM Personal Communications Multiple Vulnerabilities(ibm10717437)	Vulnerability - level 4	Vuln
371160	F5 BIG-IP Application Security Manager (ASM) Open Secure Sockets Layer (OpenSSL) Denial Of Service (DoS) Vulnerability (K21665601)	Vulnerability - level 3	Vuln
371174	TeamViewer Brute Force Authentication Bypass Vulnerability	Vulnerability - level 3	Vuln
371180	IBM Java SDK Multiple Vulnerabilities (Oracle July 17 2018 CPU (1.6.0_201, 1.7.0_191, 1.8.0_181))	Vulnerability - level 4	Vuln
371190	IBM WebSphere Application Server Multiple Vulnerabilities (swg22016214)	Vulnerability - level 4	Practice
371195	IBM Websphere Portal Apache Struts Remote Code Execution Vulnerability(swg21988770)	Vulnerability - level 4	Vuln
371198	IBM WebSphere Portal Multiple Vulnerabilities (swg22001394)	Vulnerability - level 3	Vuln
371218	Apple macOS Mojave 10.14 Not Installed (APPLE-SA-2018-9-24-1)	Vulnerability - level 5	Vuln
371226	Delta Electronics PMSOFT Out-Of-Bounds Read Vulnerability	Vulnerability - level 3	Vuln
371266	Oracle VM VirtualBox Multiple Vulnerabilities (CPUOCT2018)	Vulnerability - level 3	Vuln
371278	Delta Industrial Automation TPEditor Multiple Vulnerabilities	Vulnerability - level 4	Vuln
371290	Advantech WebAccess Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
371291	Apple macOS Mojave 10.14.1, Security Update 2018-002 High Sierra, Security Update 2018-005 Sierra Not Installed (HT209193)	Vulnerability - level 5	Vuln
371349	F5 BIG-IP ASM,LTM,APM OpenSSH Privilege Escalation Vulnerability (K62201745)	Vulnerability - level 4	Vuln
371375	Omron CX-One Multiple Vulnerabilities	Vulnerability - level 3	Vuln

371387	F5 BIG-IP ASM,LTM,APM NTP Multiple Vulnerabilities (K07082049,K99254031,K32262483)	Vulnerability - level 3	Vuln
371397	IBM Cognos Business Intelligence Multiple Security Vulnerabilities(swg22014202)	Vulnerability - level 5	Vuln
371401	Cisco UCS 6200 Series Fabric Interconnects Multiple Vulnerabilities in Network Time Protocol Daemon (CSCuz92668)	Vulnerability - level 4	Vuln
371402	Cisco UCS 6200 Series Fabric Interconnects Multiple Vulnerabilities in Network Time Protocol Daemon (CSCvc23476)	Vulnerability - level 3	Vuln
371530	McAfee ePolicy Orchestrator Open Secure Sockets Layer (OpenSSL) Vulnerability (SB10165)	Vulnerability - level 3	Vuln
371633	F5 BIG-IP ASM,LTM,APM BIND Denial Of Service Vulnerability (K95343321)	Vulnerability - level 3	Vuln
371671	FlexNet Publisher Remote Code Execution Vulnerability (SA85979)	Vulnerability - level 3	Vuln
371706	UltraVNC Multiple Code Execution Vulnerabilities	Vulnerability - level 4	Vuln
371716	F5 BIG-IP Access Policy Manager (APM), Application Security Manager (ASM), Local Traffic Manager (LTM) Open Secure Sockets Layer (OpenSSL) Vulnerability (K21462542)	Vulnerability - level 3	Vuln
371788	UltraVNC multiple out-of-bounds access vulnerabilities	Vulnerability - level 4	Vuln
371905	FreeBSD Security Update for rssh - multiple vulnerabilities (d193aa9f-3f8c-11e9-9a24-6805ca0b38e8)	Vulnerability - level 3	Vuln
371915	FreeBSD Security Update for Django -- AdminURLFieldWidget XSS (ffc73e87-87f0-11e9-ad56-fcaa147e860e)	Vulnerability - level 3	Vuln
371963	FreeBSD Security Update for node.js -- multiple vulnerabilities (0904e81f-a89d-11e8-afbb-bc5ff4f77b71)	Vulnerability - level 3	Vuln
372160	Teamviewer Windows Privilege Escalation vulnerability	Vulnerability - level 3	Vuln
372162	Oracle WebLogic Server Multiple Vulnerabilities (CPUOCT2019) (WebLogic Server Unix Authentication Record)	Vulnerability - level 4	Vuln
372254	Siemens LOGO! Soft Comfort Missing Integrity Verification Vulnerability(SSA-888929)	Vulnerability - level 3	Vuln
372255	TightVNC Multiple Vulnerabilities	Vulnerability - level 5	Vuln
372276	Mozilla Firefox and Firefox ESR Multiple Vulnerabilities (MFSA 2019-36,MFSA 2019-37)	Vulnerability - level 5	Vuln
372277	Mozilla Thunderbird Multiple Vulnerabilities (MFSA 2019-38)	Vulnerability - level 5	Vuln
372311	Oracle JDeveloper and ADF Remote Security Vulnerability	Vulnerability - level 4	Vuln
372332	Oracle PeopleSoft Enterprise PeopleTools Multiple vulnerabilities (CPUJAN2020)	Vulnerability - level 3	Vuln
372365	Google Chrome Prior To 80.0.3987.87 Multiple Vulnerabilities	Vulnerability - level 4	Vuln
372371	Microsoft Edge Based On Chromium Prior to 80.0.361.48 Multiple Vulnerabilities (ADV200002)	Vulnerability - level 3	Vuln
372542	Oracle VM VirtualBox Multiple Vulnerabilities (CPUOCT2019)	Vulnerability - level 3	Vuln
372648	Apache Subversion Multiple Vulnerabilities	Vulnerability - level 3	Vuln
372650	Mozilla Firefox/Thunderbird/SeaMonkey Arbitrary Code Execution Vulnerability	Vulnerability - level 4	Vuln
372656	Pidgin Out-of-bounds Write Vulnerability	Vulnerability - level 4	Vuln
372659	LibreOffice Multiple Vulnerabilities	Vulnerability - level 3	Vuln
372660	LibreOffice XML Entity Expansion Vulnerability	Vulnerability - level 3	Vuln
372661	LibreOffice(prior to 3.5.3) Multiple Vulnerabilities	Vulnerability - level 3	Vuln
372662	LibreOffice buffer overflow Vulnerability	Vulnerability - level 3	Vuln
372702	FreeBSD Security Update for MySQL Server (21d59ea3-8559-11ea-a5e2-d4c9ef517024)	Vulnerability - level 3	Vuln
372729	FreeBSD Security Update for MySQL (a6cf65ad-37d2-11ea-a1c7-b499baebfeaf)	Vulnerability - level 3	Vuln
372742	FreeBSD Security Update for Gitlab (e8483115-8b8e-11ea-bdcf-001b217b3468)	Vulnerability - level 3	Vuln
372895	IBM MQ Application Denial of Service Vulnerability	Vulnerability - level 3	Vuln
372903	EulerOS Security Update for libvncserver (EulerOS-SA-2020-1683)	Vulnerability - level 4	Vuln
372953	EulerOS Security Update for kernel (EulerOS-SA-2020-1674)	Vulnerability - level 5	Vuln
372957	EulerOS Security Update for libxml2 (EulerOS-SA-2020-1670)	Vulnerability - level 3	Vuln

372984	EulerOS Security Update for nss-softokn (EulerOS-SA-2020-1651)	Vulnerability - level 2	Vuln
372988	EulerOS Security Update for qemu-kvm (EulerOS-SA-2020-1647)	Vulnerability - level 5	Vuln
372998	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL098e) (EulerOS-SA-2020-1637)	Vulnerability - level 3	Vuln
373012	EulerOS Security Update for sqlite (EulerOS-SA-2020-1624)	Vulnerability - level 4	Vuln
373069	EulerOS Security Update for subversion (EulerOS-SA-2020-1513)	Vulnerability - level 3	Vuln
373090	EulerOS Security Update for sqlite (EulerOS-SA-2020-1434)	Vulnerability - level 3	Vuln
373136	FreeBSD Security Update for Node.js -- June 2020 Security Releases (11fca8f-ac64-11ea-9dab-000d3ab229d6)	Vulnerability - level 3	Vuln
373172	FreeBSD Security Update for mediawiki (3c5a4fe0-9ebb-11e9-9169-fcaa147e860e)	Vulnerability - level 4	Vuln
373227	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (9e0c6f7a-d46d-11e9-a1c7-b499baebfeaf)	Vulnerability - level 3	Vuln
373248	FreeBSD Security Update for sqlite3 (c4ac9c79-ab37-11ea-8b5e-b42e99a1b9c3)	Vulnerability - level 2	Vuln
373287	FreeBSD Security Update for curl (f4d638b9-e6e5-4dbe-8c70-571dbc116174)	Vulnerability - level 5	Vuln
373300	FreeBSD Security Update for nghttp2 (4bb56d2f-a5b0-11ea-a860-08002728f74c)	Vulnerability - level 3	Vuln
373335	TeamViewer Desktop Unquoted URI Handler Vulnerability	Vulnerability - level 4	Vuln
373376	FreeBSD Security Update for jasper (006e3b7c-d7d7-11e5-b85f-0018fe623f2b)	Vulnerability - level 4	Vuln
373377	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (00b0d8cd-7097-11e2-98d9-003067c2616f)	Vulnerability - level 1	Vuln
373379	FreeBSD Security Update for mantis (00d6040a-b8e0-11dd-a578-0030843d3802)	Vulnerability - level 2	Vuln
373513	Node.js Multiple Security Vulnerabilities (September 2020)	Vulnerability - level 3	Vuln
373611	EulerOS Security Update for sqlite (EulerOS-SA-2020-1300)	Vulnerability - level 3	Vuln
373622	EulerOS Security Update for libxml2 (EulerOS-SA-2020-1310)	Vulnerability - level 3	Vuln
373661	EulerOS Security Update for ImageMagick (EulerOS-SA-2020-1390)	Vulnerability - level 4	Vuln
373680	EulerOS Security Update for libxml2 (EulerOS-SA-2020-1408)	Vulnerability - level 3	Vuln
373691	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL098e) (EulerOS-SA-2020-1420)	Vulnerability - level 3	Vuln
373729	EulerOS Security Update for kernel (EulerOS-SA-2020-1807)	Vulnerability - level 4	Vuln
373733	EulerOS Security Update for libvncserver (EulerOS-SA-2020-1811)	Vulnerability - level 3	Vuln
373737	EulerOS Security Update for nghttp2 (EulerOS-SA-2020-1815)	Vulnerability - level 3	Vuln
373749	EulerOS Security Update for sqlite (EulerOS-SA-2020-1827)	Vulnerability - level 2	Vuln
373777	EulerOS Security Update for grub2 (EulerOS-SA-2020-1853)	Vulnerability - level 2	Vuln
373790	EulerOS Security Update for libvncserver (EulerOS-SA-2020-1866)	Vulnerability - level 4	Vuln
373825	EulerOS Security Update for libvncserver (EulerOS-SA-2020-1925)	Vulnerability - level 4	Vuln
373840	EulerOS Security Update for libvncserve (EulerOS-SA-2020-1940)	Vulnerability - level 3	Vuln
373851	EulerOS Security Update for sqlite (EulerOS-SA-2020-2059)	Vulnerability - level 3	Vuln
373868	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL098e) (EulerOS-SA-2020-2076)	Vulnerability - level 2	Vuln
373895	EulerOS Security Update for nss (EulerOS-SA-2020-2100)	Vulnerability - level 2	Vuln
373911	EulerOS Security Update for libvncserver (EulerOS-SA-2020-2116)	Vulnerability - level 4	Vuln
373915	OpenLDAP NULL Pointer Dereference Vulnerability	Vulnerability - level 3	Vuln
374067	Gentoo Linux libuv Buffer Overflow Vulnerability (GLSA 202009-15)	Vulnerability - level 2	Vuln
374069	Gentoo Linux gpsd Arbitrary Code Execution Vulnerability (GLSA 202009-17)	Vulnerability - level 3	Vuln
374074	Gentoo Linux libxml2 Multiple vulnerabilities (GLSA 202010-04)	Vulnerability - level 3	Vuln
374108	Apple iTunes for Windows Prior to 12.10.9 Multiple Vulnerabilities (HT211952)	Vulnerability - level 4	Vuln
374115	Gentoo Linux rssh Multiple Vulnerabilities (GLSA 202007-29)	Vulnerability - level 4	Vuln
374118	Gentoo Linux SQLite Multiple Vulnerabilities (GLSA 202007-26)	Vulnerability - level 4	Vuln

374122	Gentoo Linux Libreswan Denial Of Service Vulnerability (GLSA 202007-21)	Vulnerability - level 3	Vuln
374155	EulerOS Security Update for sqlite (EulerOS-SA-2020-1033)	Vulnerability - level 4	Vuln
374218	EulerOS Security Update for libxml2 (EulerOS-SA-2020-1117)	Vulnerability - level 3	Vuln
374222	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL098e) (EulerOS-SA-2020-1121)	Vulnerability - level 2	Vuln
374233	EulerOS Security Update for sqlite (EulerOS-SA-2020-1132)	Vulnerability - level 3	Vuln
374268	EulerOS Security Update for libxml2 (EulerOS-SA-2020-1165)	Vulnerability - level 3	Vuln
374286	EulerOS Security Update for sqlite (EulerOS-SA-2020-1180)	Vulnerability - level 3	Vuln
374331	Nagios XI 5.x Have Multiple Vulnerabilities	Vulnerability - level 3	Vuln
374396	EulerOS Security Update for libvncserver (EulerOS-SA-2020-2362)	Vulnerability - level 3	Vuln
374407	EulerOS Security Update for ntp (EulerOS-SA-2020-2374)	Vulnerability - level 4	Vuln
374428	EulerOS Security Update for sqlite (EulerOS-SA-2020-2398)	Vulnerability - level 3	Vuln
374463	EulerOS Security Update for kernel (EulerOS-SA-2020-2485)	Vulnerability - level 1	Vuln
374474	EulerOS Security Update for kernel (EulerOS-SA-2020-2498)	Vulnerability - level 1	Vuln
374492	Wibu-Systems CodeMeter Runtime Improper Input Validation Vulnerability.	Vulnerability - level 3	Vuln
374493	Wibu-Systems CodeMeter Runtime Multiple Security Vulnerabilities	Vulnerability - level 3	Vuln
374494	Wibu-Systems CodeMeter Improper Signature Verification Vulnerability	Vulnerability - level 3	Vuln
374495	Wibu-Systems CodeMeter Runtime Heap Exploitation	Vulnerability - level 3	Vuln
374566	Apple macOS Big Sur Security Update Not Installed (HT211931)	Vulnerability - level 4	Vuln
374605	Gentoo Linux Mozilla Network Security Service Multiple Vulnerabilities (GLSA 202003-37)	Vulnerability - level 3	Vuln
374607	Gentoo Linux ProFTPD Multiple Vulnerabilities (GLSA 202003-35)	Vulnerability - level 5	Vuln
374624	Gentoo Linux SQLite Multiple Vulnerabilities (GLSA 202003-16)	Vulnerability - level 3	Vuln
374631	Gentoo Linux Mozilla Thunderbird Multiple Vulnerabilities (GLSA 202003-10)	Vulnerability - level 4	Vuln
374637	Gentoo Linux Mozilla Firefox Multiple Vulnerabilities (GLSA 202003-02)	Vulnerability - level 4	Vuln
374646	F5 BIG-IP ASM,LTM,APM QEMU Vulnerability (K09081535, K41301038, K92451315)	Vulnerability - level 3	Vuln
374647	Apple iCloud for Windows Prior to 11.5 Multiple Vulnerabilities(HT211935)	Vulnerability - level 4	Vuln
374654	EulerOS Security Update for vino (EulerOS-SA-2020-2569)	Vulnerability - level 3	Vuln
374663	EulerOS Security Update for pki-core (EulerOS-SA-2020-2560)	Vulnerability - level 2	Vuln
374675	EulerOS Security Update for libvncserver (EulerOS-SA-2020-2552)	Vulnerability - level 3	Vuln
374691	Gentoo Linux Mozilla Products Multiple Vulnerabilities (GLSA 201605-06)	Vulnerability - level 3	Vuln
374693	Gentoo Linux NTP Multiple Vulnerabilities (GLSA 201607-15)	Vulnerability - level 3	Vuln
374695	Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 201612-16)	Vulnerability - level 3	Vuln
374696	Gentoo Linux OpenSSH Multiple Vulnerabilities (GLSA 201612-18)	Vulnerability - level 3	Vuln
374703	Gentoo Linux Apache Tomcat Multiple Vulnerabilities (GLSA 201705-09)	Vulnerability - level 3	Vuln
374741	EulerOS Security Update for kernel (EulerOS-SA-2020-2514)	Vulnerability - level 4	Vuln
374745	EulerOS Security Update for libvncserver (EulerOS-SA-2020-2518)	Vulnerability - level 4	Vuln
374774	Gentoo Linux Open Secure Sockets Layer (OpenSSL) Denial of Service (DoS) Vulnerability (GLSA 202012-13)	Vulnerability - level 2	Vuln
374775	Gentoo Linux cURL Multiple Vulnerabilities (GLSA 202012-14)	Vulnerability - level 3	Vuln
374793	Apple macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave (HT212147)	Vulnerability - level 4	Vuln
374852	EulerOS Security Update for kernel (EulerOS-SA-2021-1009)	Vulnerability - level 4	Vuln
374856	Gentoo Linux Python Multiple Vulnerabilities (GLSA 202003-26)	Vulnerability - level 3	Vuln
374867	Gentoo Linux NodeJS Multiple Vulnerabilities (GLSA 202101-07)	Vulnerability - level 5	Vuln
374875	Oracle PeopleSoft Enterprise PeopleTools Multiple vulnerabilities (CPUJAN2021)	Vulnerability - level 3	Vuln
374898	Gentoo Linux Dnsmasq Multiple Vulnerabilities (GLSA 202101-17)	Vulnerability - level 2	Vuln

374920	Node.js Open Secure Sockets Layer (OpenSSL) Vulnerability	Vulnerability - level 2	Vuln
374922	EulerOS Security Update for open-iscsi (EulerOS-SA-2021-1012)	Vulnerability - level 3	Vuln
374923	EulerOS Security Update for openldap (EulerOS-SA-2021-1013)	Vulnerability - level 3	Vuln
374924	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1014)	Vulnerability - level 2	Vuln
374938	EulerOS Security Update for kernel (EulerOS-SA-2021-1028)	Vulnerability - level 4	Vuln
374941	EulerOS Security Update for open-iscsi (EulerOS-SA-2021-1031)	Vulnerability - level 3	Vuln
374942	EulerOS Security Update for openldap (EulerOS-SA-2021-1032)	Vulnerability - level 3	Vuln
374943	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1033)	Vulnerability - level 2	Vuln
374951	EulerOS Security Update for bzip2 (EulerOS-SA-2021-1060)	Vulnerability - level 5	Vuln
374971	EulerOS Security Update for iscsi-initiator-utils (EulerOS-SA-2021-1076)	Vulnerability - level 3	Vuln
374983	EulerOS Security Update for libvncserver (EulerOS-SA-2021-1091)	Vulnerability - level 4	Vuln
374994	EulerOS Security Update for nss (EulerOS-SA-2021-1102)	Vulnerability - level 3	Vuln
374995	EulerOS Security Update for openldap (EulerOS-SA-2021-1103)	Vulnerability - level 3	Vuln
374996	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1104)	Vulnerability - level 2	Vuln
375016	EulerOS Security Update for subversion (EulerOS-SA-2021-1124)	Vulnerability - level 2	Vuln
375021	EulerOS Security Update for vino (EulerOS-SA-2021-1129)	Vulnerability - level 3	Vuln
375034	EulerOS Security Update for dnsmasq (EulerOS-SA-2021-1138)	Vulnerability - level 4	Vuln
375049	EulerOS Security Update for libvncserver (EulerOS-SA-2021-1153)	Vulnerability - level 3	Vuln
375053	EulerOS Security Update for openldap (EulerOS-SA-2021-1157)	Vulnerability - level 3	Vuln
375056	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1160)	Vulnerability - level 2	Vuln
375095	Tenable Nessus Multiple Vulnerabilities (TNS-2020-12)	Vulnerability - level 3	Vuln
375133	EulerOS Security Update for openldap (EulerOS-SA-2021-1269)	Vulnerability - level 3	Vuln
375139	EulerOS Security Update for dnsmasq (EulerOS-SA-2021-1263)	Vulnerability - level 4	Vuln
375152	EulerOS Security Update for openldap (EulerOS-SA-2021-1250)	Vulnerability - level 3	Vuln
375158	EulerOS Security Update for dnsmasq (EulerOS-SA-2021-1244)	Vulnerability - level 4	Vuln
375166	EulerOS Security Update for subversion (EulerOS-SA-2021-1235)	Vulnerability - level 2	Vuln
375181	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL098e) (EulerOS-SA-2021-1221)	Vulnerability - level 3	Vuln
375184	EulerOS Security Update for nss (EulerOS-SA-2021-1218)	Vulnerability - level 2	Vuln
375194	EulerOS Security Update for libvncserver (EulerOS-SA-2021-1208)	Vulnerability - level 4	Vuln
375201	F5 BIG-IP ASM,LTM,APM Linux Kernel Vulnerability (K82356391)	Potential Vulnerability - level 3	Practice
375205	FreeBSD Security Update for Open Secure Sockets Layer (OpenSSL) (96a21236-707b-11eb-96d8-d4c9ef517024)	Vulnerability - level 4	Vuln
375221	EulerOS Security Update for dnsmasq (EulerOS-SA-2021-1374)	Vulnerability - level 4	Vuln
375225	EulerOS Security Update for vino (EulerOS-SA-2021-1370)	Vulnerability - level 3	Vuln
375230	EulerOS Security Update for subversion (EulerOS-SA-2021-1365)	Vulnerability - level 2	Vuln
375249	EulerOS Security Update for pki-core (EulerOS-SA-2021-1346)	Vulnerability - level 3	Vuln
375256	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL110f) (EulerOS-SA-2021-1339)	Vulnerability - level 2	Vuln
375257	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1338)	Vulnerability - level 2	Vuln
375258	EulerOS Security Update for openldap (EulerOS-SA-2021-1337)	Vulnerability - level 3	Vuln
375274	EulerOS Security Update for libvncserver (EulerOS-SA-2021-1321)	Vulnerability - level 4	Vuln
375288	EulerOS Security Update for iscsi-initiator-utils (EulerOS-SA-2021-1307)	Vulnerability - level 3	Vuln
375307	EulerOS Security Update for dnsmasq (EulerOS-SA-2021-1288)	Vulnerability - level 4	Vuln
375312	EulerOS Security Update for bzip2 (EulerOS-SA-2021-1283)	Vulnerability - level 5	Vuln
375337	IBM Spectrum Control Multiple Vulnerabilities (6415993)	Vulnerability - level 4	Vuln
375350	EulerOS Security Update for bzip2 (EulerOS-SA-2021-1180)	Vulnerability - level 5	Vuln
375370	EulerOS Security Update for kernel (EulerOS-SA-2021-1200)	Vulnerability - level 4	Vuln
375425	Oracle BI Publisher Multiple Vulnerabilities(CPUOCT2020)	Vulnerability - level 3	Vuln
375442	HPE System Management Homepage Multiple Vulnerabilities (HPESBMU03593)	Vulnerability - level 4	Vuln

375444	IBM Spectrum Control Node js Vulnerability(6261327)	Vulnerability - level 5	Vuln
375467	Node.js Multiple Vulnerabilities (February 2021)	Vulnerability - level 3	Vuln
375482	Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUAPR2021)	Vulnerability - level 4	Vuln
375503	Apple MacOS Big Sur 11.3 Not Installed (HT212325)	Vulnerability - level 4	Vuln
375507	Apple macOS Security Update 2021-002 Catalina (HT212326)	Vulnerability - level 5	Vuln
375510	Apple macOS Security Update 2021-003 Mojave (HT212327)	Vulnerability - level 4	Vuln
375520	Mysql Workbench Critical Patch Update April 2021	Vulnerability - level 3	Vuln
375585	Apple macOS Security Update 2021-004 Mojave (HT212531)	Vulnerability - level 4	Vuln
375586	Apple macOS Security Update 2021-003 Catalina (HT212530)	Vulnerability - level 4	Vuln
375587	Apple Safari Multiple Vulnerabilities (HT212534)	Vulnerability - level 3	Vuln
375588	Apple MacOS Big Sur 11.4 Not Installed (HT212529)	Vulnerability - level 4	Vuln
375591	F5 BIG-IP BIND Vulnerability (K11426315)	Potential Vulnerability - level 2	Practice
375626	IBM Cognos Analytics Multiple Vulnerabilities (6451705)	Vulnerability - level 4	Vuln
375658	Node.js Multiple Vulnerabilities (February 2021) (Installed with Nodlist)	Vulnerability - level 3	Vuln
375664	F5 BIG-IP ASM,LTM,APM BIG-IP BIND Vulnerability (K96223611)	Vulnerability - level 4	Vuln
375670	IBM WebSphere Application Server Multiple Vulnerabilities (6453091)	Vulnerability - level 3	Practice
375746	Apple MacOS Big Sur 11.5 Not Installed (HT212602)	Vulnerability - level 4	Vuln
375772	PostgreSQL Have Multiple Vulnerabilities	Vulnerability - level 3	Vuln
375786	Node.js Remote Code Execution Vulnerability Aug 2021	Vulnerability - level 3	Vuln
375800	Autodesk AutoCAD Multiple Vulnerabilities (adsk-sa-2021-0004)	Vulnerability - level 3	Vuln
375828	Node.js Multiple Vulnerabilities (August 2021)	Vulnerability - level 4	Vuln
375877	Kibana Multiple Security Vulnerabilities (ESA-2021-21, ESA-2021-22, ESA-2021-24)	Vulnerability - level 4	Vuln
375890	Node.js Memory Corruption Vulnerability July 2021	Vulnerability - level 3	Vuln
375955	IBM Security SiteProtector System Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities	Vulnerability - level 3	Vuln
375956	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Open Secure Sockets Layer (OpenSSL) Vulnerability (K19559038)	Vulnerability - level 3	Vuln
375963	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Apache HTTPD Vulnerability (K72382141)	Vulnerability - level 3	Vuln
375964	Oracle Java SE Critical Patch Update - October 2021 (CPUOCT2021)	Vulnerability - level 4	Vuln
375965	Oracle Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (CPUOCT2021)	Vulnerability - level 4	Vuln
375971	Nmap Buffer Overrun Vulnerability	Vulnerability - level 3	Vuln
375988	Apache Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (DEPRECATED)	Potential Vulnerability - level 4	Practice
376039	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Open Secure Sockets Layer (OpenSSL) Vulnerability (K42910051)	Potential Vulnerability - level 3	Practice
376041	IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6493841)	Potential Vulnerability - level 3	Practice
376044	BusyBox Denial of Service (DoS) Vulnerability	Vulnerability - level 3	Vuln
376048	BusyBox Denial of Service (DoS) Vulnerability	Vulnerability - level 3	Vuln
376049	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) BIND Vulnerability (K77326807)	Potential Vulnerability - level 3	Practice
376053	F5 BIG-IP Local Traffic Manager (LTM), Access Policy Manager (APM), Application Security Manager (ASM) cURL Vulnerability (K63525058)	Potential Vulnerability - level 2	Practice
376054	BusyBox Denial of Service (DoS) Vulnerability	Vulnerability - level 3	Vuln
376057	GoLang Multiple Vulnerabilities	Vulnerability - level 3	Vuln

376060	F5 BIG-IP Application Security Manager (ASM), Access Policy Manager (APM), Local Traffic Manager (LTM) Python Vulnerability (K57542514)	Potential Vulnerability - level 3	Practice
376087	Azul Java Multiple Vulnerabilities Security Update October 2021	Vulnerability - level 5	Vuln
376088	BusyBox Use After Free Vulnerability	Vulnerability - level 3	Vuln
376114	IBM Integration Bus Node.js Vulnerability (6515532,6516066)	Vulnerability - level 3	Vuln
376204	Mysql Workbench Critical Patch Update Oct 2021	Vulnerability - level 5	Vuln
376248	IBM Spectrum Control Multiple Vulnerabilities (6359903,6359899,6359901)	Vulnerability - level 3	Vuln
376257	Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUJAN2022)	Vulnerability - level 5	Vuln
376363	Oracle MYSQL Connector/ODBC Critical Patch Update (CPU) January 2022 (CPUJAN2022)	Vulnerability - level 4	Vuln
376381	IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6493845,6493841)	Vulnerability - level 4	Vuln
376409	Abyss Web Server Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Engine Vulnerability	Vulnerability - level 3	Vuln
376533	Spring Framework Denial of Service (DoS) Vulnerability	Vulnerability - level 3	Vuln
376544	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Open Secure Sockets Layer (OpenSSL) Vulnerability (K24624116)	Potential Vulnerability - level 4	Practice
376547	Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUAPR2022)	Vulnerability - level 4	Vuln
376550	Oracle Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (CPUAPR2022)	Vulnerability - level 3	Vuln
376567	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Linux kernel Vulnerability (K09604370)	Potential Vulnerability - level 4	Practice
376579	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Expat Vulnerability (K91589041)	Potential Vulnerability - level 4	Practice
376581	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Expat Vulnerability (K23421535)	Potential Vulnerability - level 4	Practice
376583	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Expat Vulnerability (K19473898)	Potential Vulnerability - level 3	Practice
376607	Apple macOS Security Update 2022-004 Catalina (HT213255)	Vulnerability - level 5	Vuln
376608	Apple MacOS Big Sur 11.6.6 Not Installed (HT213256)	Vulnerability - level 5	Vuln
376612	Apple macOS Monterey 12.4 Not Installed (HT213257)	Vulnerability - level 5	Vuln
376629	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) TMM Vulnerability (K41440465)	Vulnerability - level 4	Vuln
376658	F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Apache Hypertext Transfer Protocol Server (HTTP Server) Vulnerability (K67090077)	Potential Vulnerability - level 3	Practice
376730	Node.js Multiple Vulnerabilities (JULY 2022)	Vulnerability - level 4	Vuln
376863	IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6595149)	Vulnerability - level 3	Vuln
376865	IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6565413)	Vulnerability - level 3	Vuln
376869	Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2021:0011)	Vulnerability - level 4	Vuln
376880	Alibaba Cloud Linux Security Update for postgresql (ALINUX2-SA-2021:0041)	Vulnerability - level 4	Vuln
376911	Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX2-SA-2020:0197)	Vulnerability - level 4	Vuln
376918	Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2021:0006)	Vulnerability - level 4	Vuln

376925	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125)	Vulnerability - level 4	Vuln
376933	Alibaba Cloud Linux Security Update for microcode_ctl (ALINUX3-SA-2021:0040)	Vulnerability - level 4	Vuln
376943	NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Disclosure of Sensitive Information Vulnerability (NTAP-20220204-0006)	Vulnerability - level 4	Vuln
376952	NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Disclosure of Sensitive Information Vulnerability (NTAP-20210625-0002,NTAP-20210716-0005)	Vulnerability - level 4	Vuln
376961	NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Disclosure of Sensitive Information Vulnerability (NTAP-20211008-0004)	Vulnerability - level 4	Vuln
376969	NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Disclosure of Sensitive Information Vulnerability (NTAP-20210122-0007)	Vulnerability - level 4	Vuln
376986	Alibaba Cloud Linux Security Update for xmlrpc-c (ALINUX3-SA-2022:0035)	Vulnerability - level 4	Vuln
377024	Alibaba Cloud Linux Security Update for python (ALINUX2-SA-2019:0020)	Vulnerability - level 4	Vuln
377031	Alibaba Cloud Linux Security Update for libvncserver (ALINUX2-SA-2020:0034)	Vulnerability - level 4	Vuln
377038	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)	Vulnerability - level 4	Vuln
377041	Alibaba Cloud Linux Security Update for expat (ALINUX2-SA-2022:0017)	Vulnerability - level 4	Vuln
377053	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2022:0028)	Vulnerability - level 4	Vuln
377078	Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2021:0026)	Vulnerability - level 4	Vuln
377088	Alibaba Cloud Linux Security Update for microcode_ctl (ALINUX2-SA-2021:0047)	Vulnerability - level 4	Vuln
377097	Alibaba Cloud Linux Security Update for expat (ALINUX3-SA-2022:0021)	Vulnerability - level 4	Vuln
377098	Alibaba Cloud Linux Security Update for postgresql:13 (ALINUX3-SA-2021:0043)	Vulnerability - level 4	Vuln
377101	Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2021:0074)	Vulnerability - level 4	Vuln
377102	Alibaba Cloud Linux Security Update for nodejs:14 (ALINUX3-SA-2021:0022)	Vulnerability - level 4	Vuln
377105	Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2022:0025)	Vulnerability - level 4	Vuln
377109	Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2021:0021)	Vulnerability - level 4	Vuln
377112	Alibaba Cloud Linux Security Update for microcode_ctl (ALINUX3-SA-2021:0057)	Vulnerability - level 4	Vuln
377117	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)	Vulnerability - level 4	Vuln
377140	Alibaba Cloud Linux Security Update for dnsmasq (ALINUX3-SA-2021:0009)	Vulnerability - level 4	Vuln
377145	Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2022:0023)	Vulnerability - level 4	Vuln
377148	Alibaba Cloud Linux Security Update for nghttp2 (ALINUX3-SA-2022:0101)	Vulnerability - level 4	Vuln
377150	Alibaba Cloud Linux Security Update for subversion:1.10 (ALINUX3-SA-2021:0018)	Vulnerability - level 4	Vuln
377151	Alibaba Cloud Linux Security Update for bind (ALINUX3-SA-2021:0025)	Vulnerability - level 4	Vuln

377157	Alibaba Cloud Linux Security Update for nodejs:14 (ALINUX3-SA-2021:0072)	Vulnerability - level 4	Vuln
377168	Alibaba Cloud Linux Security Update for nss, nss-softokn, nss-util (ALINUX2-SA-2020:0005)	Vulnerability - level 4	Vuln
377184	Alibaba Cloud Linux Security Update for libvncserver (ALINUX2-SA-2020:0111)	Vulnerability - level 4	Vuln
377193	Alibaba Cloud Linux Security Update for httpd (ALINUX2-SA-2022:0018)	Vulnerability - level 4	Vuln
377204	Alibaba Cloud Linux Security Update for microcode_ctl (ALINUX2-SA-2021:0038)	Vulnerability - level 4	Vuln
377218	Alibaba Cloud Linux Security Update for httpd (ALINUX2-SA-2022:0004)	Vulnerability - level 4	Vuln
377233	Alibaba Cloud Linux Security Update for openldap (ALINUX2-SA-2021:0023)	Vulnerability - level 3	Vuln
377255	Alibaba Cloud Linux Security Update for openldap (ALINUX2-SA-2022:0013)	Vulnerability - level 3	Vuln
377300	Alibaba Cloud Linux Security Update for nss, nss-softokn, nss-util, and nspr (ALINUX2-SA-2019:0104)	Vulnerability - level 3	Vuln
377302	Alibaba Cloud Linux Security Update for curl (ALINUX2-SA-2019:0058)	Vulnerability - level 2	Vuln
377322	Alibaba Cloud Linux Security Update for microcode_ctl (ALINUX2-SA-2020:0187)	Vulnerability - level 3	Vuln
377330	Alibaba Cloud Linux Security Update for mingw packages (ALINUX3-SA-2022:0121)	Vulnerability - level 3	Vuln
377341	Alibaba Cloud Linux Security Update for sqlite (ALINUX3-SA-2022:0111)	Vulnerability - level 3	Vuln
377345	Alibaba Cloud Linux Security Update for grub2 (ALINUX3-SA-2022:0064)	Vulnerability - level 3	Vuln
377365	Alibaba Cloud Linux Security Update for libxml2 (ALINUX3-SA-2022:0018)	Vulnerability - level 3	Vuln
377367	Alibaba Cloud Linux Security Update for grub2 (ALINUX3-SA-2021:0026)	Vulnerability - level 3	Vuln
377375	Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2022:0131)	Vulnerability - level 3	Vuln
377378	Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2022:0017)	Vulnerability - level 3	Vuln
377387	Alibaba Cloud Linux Security Update for python3 (ALINUX3-SA-2021:0080)	Vulnerability - level 3	Vuln
377396	Alibaba Cloud Linux Security Update for curl (ALINUX3-SA-2021:0078)	Vulnerability - level 3	Vuln
377408	Alibaba Cloud Linux Security Update for libxml2 (ALINUX3-SA-2021:0047)	Vulnerability - level 3	Vuln
377414	Alibaba Cloud Linux Security Update for fwupd (ALINUX3-SA-2021:0048)	Vulnerability - level 3	Vuln
377415	Alibaba Cloud Linux Security Update for libuv (ALINUX3-SA-2022:0099)	Vulnerability - level 2	Vuln
377422	Alibaba Cloud Linux Security Update for nodejs:14 (ALINUX3-SA-2022:0014)	Vulnerability - level 3	Vuln
377435	Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX2-SA-2022:0002)	Vulnerability - level 3	Vuln
377440	Alibaba Cloud Linux Security Update for curl (ALINUX2-SA-2019:0044)	Vulnerability - level 2	Vuln
377454	Alibaba Cloud Linux Security Update for libxml2 (ALINUX2-SA-2020:0149)	Vulnerability - level 3	Vuln
377475	Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX2-SA-2021:0056)	Vulnerability - level 3	Vuln
377492	Alibaba Cloud Linux Security Update for ipa (ALINUX2-SA-2020:0169)	Vulnerability - level 3	Vuln

377496	Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2021:0053)	Vulnerability - level 3	Vuln
377512	Alibaba Cloud Linux Security Update for subversion (ALINUX2-SA-2020:0144)	Vulnerability - level 3	Vuln
377533	Alibaba Cloud Linux Security Update for grub2 (ALINUX2-SA-2020:0108)	Vulnerability - level 3	Vuln
377548	Alibaba Cloud Linux Security Update for grub2 (ALINUX2-SA-2021:0020)	Vulnerability - level 3	Vuln
377551	Alibaba Cloud Linux Security Update for microcode_ctl (ALINUX2-SA-2020:0098)	Vulnerability - level 3	Vuln
377563	Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2022:0148)	Vulnerability - level 3	Vuln
377567	Alibaba Cloud Linux Security Update for gnome (ALINUX3-SA-2022:0108)	Vulnerability - level 3	Vuln
377580	Alibaba Cloud Linux Security Update for expat (ALINUX3-SA-2022:0128)	Vulnerability - level 3	Vuln
377624	Alibaba Cloud Linux Security Update for nodejs:14 (ALINUX3-SA-2022:0165)	Vulnerability - level 3	Vuln
377645	Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUOCT2022)	Vulnerability - level 3	Vuln
377648	Oracle Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities(CPUOCT2022)	Vulnerability - level 4	Vuln
377651	Oracle MySQL Connector/ODBC Critical Patch Update (CPU) October 2022 (CPUOCT2022)	Vulnerability - level 3	Vuln
377726	F5 BIG-IP Libxml2 vulnerability cve-2022-23308 (K32760744)	Potential Vulnerability - level 4	Practice
377766	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2022:0049)	Vulnerability - level 4	Vuln
377786	Alibaba Cloud Linux Security Update for mingw-expat (ALINUX3-SA-2022:0183)	Vulnerability - level 4	Vuln
377817	Alibaba Cloud Linux Security Update for pcs (ALINUX2-SA-2022:0056)	Vulnerability - level 4	Vuln
377871	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0001)	Vulnerability - level 4	Vuln
377911	Oracle Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (CPUJAN2023)	Vulnerability - level 4	Vuln
377937	Splunk Enterprise Multiple Vulnerabilities (svd-2022-0804)	Vulnerability - level 4	Vuln
377944	Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2023:0006)	Vulnerability - level 3	Vuln
377988	Citrix Virtual Apps and Desktops Privilege Escalation Vulnerability (CTX477616)	Vulnerability - level 4	Vuln
377989	Citrix Workspace App Multiple Vulnerabilities (CTX477617)	Vulnerability - level 4	Vuln
377990	Citrix Workspace App For Linux Session Takeover Vulnerability (CTX477618)	Vulnerability - level 4	Vuln
378004	Splunk Enterprise Multiple Vulnerabilities (SVD-2023-0215,SVD-2023-0211,SVD-2023-0208)	Vulnerability - level 4	Vuln
378043	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0011)	Vulnerability - level 4	Vuln
378134	Virtuozzo Linux Security Update for java-1.8.0-openjdk-debug (VZLSA-2017:1789)	Vulnerability - level 5	Vuln
378170	Virtuozzo Linux Security Update for java-1.7.0-openjdk (VZLSA-2017:2424)	Vulnerability - level 5	Vuln
378198	Virtuozzo Linux Security Update for python-test (VZLSA-2019:1467)	Vulnerability - level 4	Vuln
378199	Virtuozzo Linux Security Update for ntp (VZLSA-2017:0252)	Vulnerability - level 4	Vuln
378244	Virtuozzo Linux Security Update for wpa_supplicant (VZLSA-2017:2907)	Vulnerability - level 4	Vuln
378248	Virtuozzo Linux Security Update for wpa_supplicant (VZLSA-2017:2911)	Vulnerability - level 3	Vuln

378263	Virtuozzo Linux Security Update for microcode_ctl (VZLSA-2020:5083)	Vulnerability - level 3	Vuln
378291	Virtuozzo Linux Security Update for nss-softokn-devel (VZLSA-2019:4152)	Vulnerability - level 4	Vuln
378308	Virtuozzo Linux Security Update for java-1.7.0-openjdk-accessibility (VZLSA-2017:3392)	Vulnerability - level 5	Vuln
378336	Zimbra Collaboration Suite (ZCS) Multiple Vulnerabilities	Vulnerability - level 4	Vuln
378348	Zimbra Collaboration Multiple Vulnerabilities	Vulnerability - level 3	Vuln
378416	Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2023:0033)	Vulnerability - level 4	Vuln
378420	IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6467651)	Vulnerability - level 3	Vuln
378423	Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX2-SA-2023:0016)	Vulnerability - level 4	Vuln
378430	Oracle MySQL Connectors 8.0.x Denial of Service (DoS) Vulnerability (CPUAPR2023)	Vulnerability - level 4	Vuln
378433	Oracle Hypertext Transfer Protocol Server (HTTP Server) Server Multiple Vulnerabilities (CPUAPR2023)	Vulnerability - level 5	Vuln
378438	HCL BigFix Multiple Security Vulnerabilities (KB0103724)	Vulnerability - level 4	Vuln
378445	F5 BIG-IP Denial of Service (DoS) Vulnerability (K000132946)	Potential Vulnerability - level 4	Practice
378449	F5 BIG-IP Denial of Service (DoS) Vulnerability (K000132941)	Potential Vulnerability - level 4	Vuln
378473	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0021)	Vulnerability - level 4	Vuln
378491	NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Multiple OpenSSL Denial of Service (DoS) Vulnerabilities (NTAP-20230214-0011)	Vulnerability - level 4	Vuln
378509	Splunk Enterprise Multiple Vulnerabilities (SP-CAAAPKV)	Vulnerability - level 5	Vuln
378515	Alibaba Cloud Linux Security Update for edk2 (ALINUX3-SA-2023:0044)	Vulnerability - level 4	Vuln
378599	Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)	Vulnerability - level 5	Vuln
38002	SQLite 'SQLITE_SECURE_DELETE' Local Information Disclosure Vulnerability	Potential Vulnerability - level 3	
38002	UDP Test-Services	Potential Vulnerability - level 3	Practice
38009	Joomla! 'com_rsgallery2' Component 'catid' Parameter SQL Injection Vulnerability	Potential Vulnerability - level 3	
38009	XZERES 442SR Wind Turbine Cross-Site Request Forgery Vulnerability	Potential Vulnerability - level 3	Practice
38191	Joomla! sh404SEF Component URI Cross-Site Scripting Vulnerability	Vulnerability - level 3	
38191	OpenSSH Remote Root Authentication Timing Side-Channel Weakness	Vulnerability - level 3	Vuln
38500	Apple iTunes Unspecified Heap Overflow Vulnerability	Potential Vulnerability - level 3	Practice
38500	Cisco Digital Media Manager (CVE-2010-0571) Remote Privilege Escalation Vulnerability	Potential Vulnerability - level 3	
38501	Apple Quicktime Unspecified Heap Overflow Vulnerability	Vulnerability - level 3	Vuln
38501	Cisco Unified Communications Manager SCCP (CVE-2010-0588) Denial of Service Vulnerability	Vulnerability - level 3	
38513	Apple QuickTime Multiple Vulnerabilities (APPLE-SA-2006-01-10)	Vulnerability - level 3	Vuln
38513	Drupal AddThis Button Module HTML Injection Vulnerability	Vulnerability - level 3	
38516	CA (Computer Associates) iTechnology iGateway Service Content-Length Heap Overflow Vulnerability	Vulnerability - level 5	Vuln
38516	HazelPress 'login.php' Multiple SQL Injection Vulnerabilities	Vulnerability - level 5	
38557	OneCMS 'user' Parameter SQL Injection Vulnerability	Vulnerability - level 3	
38557	OpenSSL PKCS Padding RSA Signature Forgery Vulnerability	Vulnerability - level 3	Practice

38561	Natychmiast CMS Multiple Cross Site Scripting and SQL Injection Vulnerabilities	Vulnerability - level 4	
38561	OpenSSL Multiple Vulnerabilities	Vulnerability - level 4	Practice
38562	OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	Vulnerability - level 4	
38562	OpenVPN Multiple Vulnerabilities	Vulnerability - level 4	Vuln
38569	Symantec Veritas NetBackup Multiple Buffer Overflow Vulnerabilities	Vulnerability - level 4	Vuln
38569	VLC Media Player Bookmark Creation Buffer Overflow Vulnerability	Vulnerability - level 4	
38595	OpenSSL "SSL_get_shared_ciphers()" Off-By-One Buffer Overflow	Vulnerability - level 4	Practice
38595	Perforce P4Web Weak Session Cookie Session Hijacking Vulnerability	Vulnerability - level 4	
38601	ASPCode CMS 'default.asp' Multiple Cross Site Scripting Vulnerabilities	Vulnerability - level 3	
38601	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)	Vulnerability - level 3	Practice
38602	OpenSSL Multiple Remote Security Vulnerabilities	Potential Vulnerability - level 4	Practice
38602	QuickZip ZIP File Remote Buffer Overflow Vulnerability	Potential Vulnerability - level 4	
38607	Linux Kernel Video Output Status Local Denial of Service Vulnerability	Vulnerability - level 4	
38607	SSL Server Diffie-Hellman passive listening attack Vulnerability	Vulnerability - level 4	Practice
38608	SSL Server Diffie-Hellman Weak Encryption Vulnerability (Logjam)	Potential Vulnerability - level 4	Practice
38608	TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities	Potential Vulnerability - level 4	
38611	HP Performance Insight Remote Command Execution Vulnerability	Potential Vulnerability - level 3	
38611	OpenSSH "X SECURITY" Bypass Vulnerability	Potential Vulnerability - level 3	Practice
38620	Adcon Telemetry A840 Multiple Remote Vulnerabilities	Vulnerability - level 4	Vuln
38620	NUs 'Nus.php' SQL Injection Vulnerability	Vulnerability - level 4	
38622	MH Products kleinanzeigenmarkt 'search.php' SQL Injection Vulnerability	Vulnerability - level 3	
38622	OpenSSL Multiple Vulnerabilities (OpenSSL Security Advisory 20160301)	Vulnerability - level 3	Practice
38624	Oracle E-Business Suite Multiple Vulnerabilities (CPUOCT2015)	Potential Vulnerability - level 3	Practice
38625	OpenSSL Multiple Vulnerabilities (OpenSSL Security Advisory 20160503)	Potential Vulnerability - level 3	Practice
38625	eclime Session Fixation and Multiple Input Validation Vulnerabilities	Potential Vulnerability - level 3	
38636	Drupal Monthly Archive by Node Type Module Security Bypass Vulnerability	Potential Vulnerability - level 3	
38636	OpenSSL Multiple Vulnerabilities (OpenSSL Security Advisory 20160922)	Potential Vulnerability - level 3	Practice
38651	ImgBrowzOr 'imgbrowzOr::init()' Function Remote Directory Traversal Vulnerability	Potential Vulnerability - level 3	
38651	NTP.org ntpd Multiple Security Vulnerabilities	Potential Vulnerability - level 3	Practice
38665	Network Time Protocol Daemon ntpd Multiple Vulnerabilities	Potential Vulnerability - level 3	Practice
38679	Joomla! 'com_party' Component 'id' Parameter SQL Injection Vulnerability	Potential Vulnerability - level 4	
38679	OpenSSH Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice

38681	Joomla! 'com_gigfe' Component 'styletype' Parameter SQL Injection Vulnerability	Potential Vulnerability - level 3	
38681	Network Time Protocol Multiple Security Vulnerabilities (ntp-4.2.8p7)	Potential Vulnerability - level 3	Practice
38682	Joomla! 'com_products' Component 'intCategoryId' Parameter SQL Injection Vulnerability	Potential Vulnerability - level 3	
38682	Network Time Protocol Multiple Security Vulnerabilities (ntp-4.2.8p6)	Potential Vulnerability - level 3	Practice
38683	Apple Safari URL Schemes Handling Remote Code Execution Vulnerability	Potential Vulnerability - level 3	
38683	Network Time Protocol Multiple Security Vulnerabilities (ntp-4.2.8p5)	Potential Vulnerability - level 3	Practice
38684	Network Time Protocol Multiple Security Vulnerabilities (ntp-4.2.8p4)	Potential Vulnerability - level 4	Practice
38684	WebKit CSS 'format()' Arguments Memory Corruption Vulnerability	Potential Vulnerability - level 4	
38689	OpenSSL Buffer Overread Vulnerability (OpenSSL Security Advisory 20170828)	Potential Vulnerability - level 2	Practice
38689	WebKit Right-to-Left Displayed Text Handling Memory Corruption Vulnerability	Potential Vulnerability - level 2	
38692	OpenSSH 7.4 Not Installed Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
38692	WebKit Cross-Origin Stylesheet Request Information Disclosure Vulnerability	Potential Vulnerability - level 4	
38693	Intel Active Management Technology Multiple Remote Code Execution Vulnerabilities	Potential Vulnerability - level 4	Practice
38693	Joomla! 'com_start' Component 'mitID' Parameter SQL Injection Vulnerability	Potential Vulnerability - level 4	
38694	Intel Management Engine Multiple Privilege Escalation And Buffer Overflow Vulnerabilities	Potential Vulnerability - level 4	Practice
38694	Joomla! 'com_leader' Component 'id' Parameter SQL Injection Vulnerability	Potential Vulnerability - level 4	
38695	Joomla! 'com_family' Component 'categoryid' Parameter SQL Injection Vulnerability	Vulnerability - level 4	
38695	TLS ROBOT Vulnerability Detected	Vulnerability - level 4	Vuln
38745	Open Secure Sockets Layer (OpenSSL) Read/Write After Secure Sockets Layer (SSL) Object In Error State Vulnerability (OpenSSL Security Advisory 20171207)	Potential Vulnerability - level 2	Practice
38753	NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Multiple Vulnerabilities (NTAP-20171208-0001,NTAP-20180201-0001,NTAP-20171107-0002)	Potential Vulnerability - level 3	Practice
38753	PhpkoBo Address Book Script 'LANG_CODE' Parameter Local File Include Vulnerability	Potential Vulnerability - level 3	
38754	Joomla! 'com_route' Component 'kid' Parameter SQL Injection Vulnerability	Potential Vulnerability - level 3	
38754	NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Open Secure Shell (OpenSSH) Vulnerability (NTAP-20180201-0002)	Potential Vulnerability - level 3	Practice
38784	Joomla! 'com_include' Component 'ID_NLE' Parameter SQL Injection Vulnerability	Potential Vulnerability - level 3	
38784	Open Secure Sockets Layer (OpenSSL) Security Update (OpenSSL Security Advisory 20190910)	Potential Vulnerability - level 3	Practice
38785	Joomla! 'com_ckforms' Component 'fid' Parameter SQL Injection Vulnerability	Potential Vulnerability - level 2	
38785	Open Secure Sockets Layer (OpenSSL) Security Update (OpenSSL Security Advisory 20190730)	Potential Vulnerability - level 2	Practice
38796	Open Secure Sockets Layer (OpenSSL) Raccoon Attack Vulnerability(20200909)	Potential Vulnerability - level 3	Practice

38796	TYPO3 Simple Gallery (sk_simplegallery) Cross Site Scripting and SQL Injection Vulnerabilities	Potential Vulnerability - level 3	
38815	Pulse Connect Secure and Pulse Policy Secure Multiple Vulnerabilities (SA44601)	Potential Vulnerability - level 3	Practice
38815	VariCAD 2010 'DWB' File Remote Buffer Overflow Vulnerability	Potential Vulnerability - level 3	
38819	Open Source TCP/IP Stacks Multiple Vulnerabilities (Amnesia:33)	Vulnerability - level 4	Practice
38819	Quicksilver Forums Multiple Information Disclosure Vulnerabilities	Vulnerability - level 4	
38825	Cisco TelePresence Video Communication Server dnsmasq DNS Forwarder Vulnerability(cisco-sa-dnsmasq-dns-2021-c5mrd3g)	Potential Vulnerability - level 3	Practice
38825	TYPO3 mm_forum Extension Unspecified Cross Site Scripting Vulnerability	Potential Vulnerability - level 3	
38829	Google Chrome prior to 4.1.249.1036 Multiple Security Vulnerabilities	Potential Vulnerability - level 2	
38829	Open Secure Sockets Layer (OpenSSL) Security Update (OpenSSL Security Advisory 20210216)	Potential Vulnerability - level 2	Practice
38837	MPlayer WAV File Remote Null Pointer Dereference Vulnerability	Potential Vulnerability - level 4	
38837	Open Secure Sockets Layer (OpenSSL) Security Update (OpenSSL Security Advisory 20210325)	Potential Vulnerability - level 4	Practice
38842	Open Secure Sockets Layer (OpenSSL) Security Update (OpenSSL Security Advisory 20190910) (DEPRECATED)	Potential Vulnerability - level 2	Practice
38842	Softsaurus CMS Multiple Remote File Include Vulnerabilities	Potential Vulnerability - level 2	
38845	Pulse Connect Secure and Pulse Policy Secure Multiple Vulnerabilities (SA44846)	Potential Vulnerability - level 3	Practice
38846	Pulse Connect Secure and Pulse Policy Secure NULL Pointer Dereference (SA44676)	Potential Vulnerability - level 3	Practice
38846	chillyCMS 'admin/index.php' Cross Site Scripting Vulnerability	Potential Vulnerability - level 3	
38855	Open Secure Sockets Layer (OpenSSL) Security Update (OpenSSL Security Advisory 20210824)	Potential Vulnerability - level 4	Practice
38855	eDisplay Personal FTP Server 'USER' Command Remote Memory Corruption Vulnerability	Potential Vulnerability - level 4	
38862	NetApp Data Open Network Technology for Appliance Products (ONTAP) Denial of Service (DoS) Vulnerability (NTAP-20210303-0002)	Potential Vulnerability - level 4	Practice
38894	GraphicsMagick File Handling Remote Integer Underflow Vulnerability	Potential Vulnerability - level 4	
38894	Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
38895	Open Secure Sockets Layer (OpenSSL) Command Injection Vulnerability	Potential Vulnerability - level 5	Practice
38895	vBulletin 4.0.2 Search Cross Site Scripting Vulnerability	Potential Vulnerability - level 5	
390006	Oracle VM Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2017-0145)	Vulnerability - level 3	Vuln
390031	Oracle VM Server for x86 Security Update for jasper (OVMSA-2017-0102)	Vulnerability - level 3	Vuln
390034	Oracle VM Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2017-0105)	Vulnerability - level 3	Vuln
390035	Oracle VM Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2017-0106)	Vulnerability - level 3	Vuln
390039	Oracle VM Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2017-0057)	Vulnerability - level 3	Vuln
390042	Oracle VM Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2017-0062)	Vulnerability - level 3	Vuln

390051	Oracle VM Server for x86 Security Update for openssh (OVMSA-2017-0053)	Vulnerability - level 3	Vuln
390057	Oracle VM Server for x86 Security Update for ntp (OVMSA-2017-0038)	Vulnerability - level 3	Vuln
390071	Oracle VM Server for x86 Security Update for mysql (OVMSA-2017-0035)	Vulnerability - level 3	Vuln
390079	Oracle VM Server for x86 Security Update for ntp (OVMSA-2017-0165)	Vulnerability - level 3	Vuln
390142	Oracle VM Server for x86 Security Update for gnupg2 (OVMSA-2018-0239)	Vulnerability - level 3	Vuln
390150	Oracle VM Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2018-0256)	Vulnerability - level 3	Vuln
390165	Oracle VM Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2019-0002)	Vulnerability - level 3	Vuln
390183	Oracle Managed Virtualization (VM) Server 3.4 Open Secure Sockets Layer (OpenSSL) Security Update (OVMSA-2019-0040)	Vulnerability - level 3	Vuln
390202	Oracle VM Server for x86 Security Update for microcode_ctl(OVMSA-2020-0026)	Vulnerability - level 4	Vuln
390203	Oracle VM Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2020-0028)	Vulnerability - level 3	Vuln
390204	Oracle VM Server for x86 Security Update for xen (OVMSA-2020-0027)	Vulnerability - level 2	Vuln
390213	Oracle VM Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2020-0051)	Vulnerability - level 5	Vuln
390215	Oracle VM Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2020-0049)	Vulnerability - level 4	Vuln
390216	Oracle VM Server for x86 Security Update for microcode_ctl (OVMSA-2020-0053)	Vulnerability - level 3	Vuln
390217	Oracle Managed Virtualization (VM) Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2021-0001)	Vulnerability - level 4	Vuln
390226	Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)	Vulnerability - level 4	Vuln
390248	Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0035)	Vulnerability - level 4	Vuln
390262	Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0019)	Vulnerability - level 4	Vuln
390265	Oracle Managed Virtualization (VM) Server for x86 Security Update for microcode_ctl (OVMSA-2022-0020)	Vulnerability - level 3	Vuln
390268	Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0026)	Vulnerability - level 4	Vuln
42018	HP OpenView Network Node Manager Remote Code Execution Vulnerability	Potential Vulnerability - level 3	Practice
42018	Zemana AntiLogger 'AntiLog32.sys' Local Privilege Escalation Vulnerability	Potential Vulnerability - level 3	
42024	HP OpenView Network Node Manager Multiple Remote Code Execution Vulnerabilities	Potential Vulnerability - level 5	Practice
42024	MediaWiki 'profileinfo.php' Cross Site Scripting Vulnerability	Potential Vulnerability - level 5	
42027	HP OpenView Network Node Manager Java JDK / JRE Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
42027	nuBuilder 'report.php' Remote File Include Vulnerability	Potential Vulnerability - level 4	
42035	OpenSSL Multiple Vulnerabilities (OpenSSL Security Advisory 20160128)	Vulnerability - level 4	Practice
42035	WebKit CVE-2010-1783 Remote Memory Corruption Vulnerability	Vulnerability - level 4	
42041	Detection of certificates with vulnerable keys 1 (ROCA)	Vulnerability - level 4	Practice
42041	WebKit 'use' Element Handling Remote Memory Corruption Vulnerability	Vulnerability - level 4	

42042	Detection of certificates with vulnerable keys 2 (ROCA)	Vulnerability - level 4	Practice
42042	WebKit Regular Expression Handling Remote Memory Corruption Vulnerability	Vulnerability - level 4	
42043	Detection of vulnerable SSH host keys 1 (ROCA)	Vulnerability - level 4	Vuln
42043	WebKit Just-In-Time Compiled JavaScript Stubs Remote Code Execution Vulnerability	Vulnerability - level 4	
42044	Detection of vulnerable SSH host keys 2 (ROCA)	Vulnerability - level 4	Vuln
42044	WebKit Element Focus Use-After-Free Remote Code Execution Vulnerability	Vulnerability - level 4	
42342	Adobe ColdFusion CVE-2010-2861 Unspecified Directory Traversal Vulnerability	Potential Vulnerability - level 3	
42342	HP OpenView Network Node Manager Remote Code Execution Vulnerability (HPSBMA02558)	Potential Vulnerability - level 3	Practice
42354	Adobe Flash Media Server (CVE-2010-2218) Remote Denial of Service Vulnerability	Potential Vulnerability - level 3	
42354	OpenSSL TLS Server Extension Parsing Race Condition Vulnerability	Potential Vulnerability - level 3	Practice
42362	Adobe Flash Player and AIR (CVE-2010-2216) Unspecified Memory Corruption Vulnerability	Potential Vulnerability - level 3	
42362	OpenSSL Ciphersuite Downgrade Security Vulnerability	Potential Vulnerability - level 3	Practice
42396	CODESYS Remote Unauthenticated Access to Command-Line	Vulnerability - level 5	Vuln
42397	Asterisk Multiple Denial of Service Vulnerabilities (AST-2012-014, AST-2012-015)	Vulnerability - level 3	Vuln
42397	Drupal 'Printer, e-mail and PDF versions' Module Local File Access Information Disclosure Weakness	Vulnerability - level 3	
42398	Drupal GovDelivery Integration Module Cross Site Scripting Vulnerability	Potential Vulnerability - level 3	
42398	OpenSSL Multiple Vulnerabilities	Potential Vulnerability - level 3	Practice
42402	InduSoft Web Studio Multiple Remote Code Execution Vulnerabilities	Vulnerability - level 5	Vuln
42421	OpenSSL Multiple Denial of Service Vulnerabilities	Potential Vulnerability - level 3	Practice
42422	Schneider SCADA Expert ClearSCADA DNP3 Driver Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
42431	OpenSSL Use-After-Free Memory Corruption Vulnerability	Potential Vulnerability - level 3	Practice
42434	OpenSSL Multiple Vulnerabilities (OpenSSL Security Advisory 20140806)	Potential Vulnerability - level 3	Practice
42434	Sonique '.xpl' File Remote Stack-Based Buffer Overflow Vulnerability	Potential Vulnerability - level 3	
42439	OpenSSL Multiple Vulnerabilities (OpenSSL Security Advisory 20150108)	Potential Vulnerability - level 3	Practice
42440	Juniper Junos Space Multiple Vulnerabilities (JSA10627)	Potential Vulnerability - level 4	Practice
42440	WordPress 'wp-admin/plugins.php' Cross Site Scripting Vulnerability	Potential Vulnerability - level 4	
43028	Cisco IOS NTP Multiple Vulnerabilities (cisco-sa-20150408-ntpd)	Vulnerability - level 4	Practice
43045	Cisco IOS ntpd Multiple Vulnerabilities (cisco-sa-20151021-ntp)	Vulnerability - level 4	Practice
43046	Cisco Nexus ntpd multiple vulnerabilities (cisco-sa-20151021-ntp)	Vulnerability - level 4	Vuln
43154	Cisco IOS Software WebVPN and SSLVPN Vulnerabilities (cisco-sa-20090325-webvpn)	Vulnerability - level 3	Vuln
43156	Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability (cisco-sa-20090325-tcp)	Vulnerability - level 3	Vuln
43310	Juniper JUNOS Multiple Vulnerabilities in OpenSSL (JSA10575)	Vulnerability - level 3	Vuln
43314	Siemens SCALANCE X-200 Series Switches Authentication Bypass	Vulnerability - level 3	Vuln

43333	Juniper Network Operating System (Junos OS) Secure Sockets Layer/Transport Layer Security (SSL/TLS) Renegotiation Denial of Service (DoS) Vulnerability (JSA10580)	Vulnerability - level 3	Vuln
43349	RuggedCom ROS Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
43357	Sierra Wireless AirLink Raven X Multiple Security Issues	Potential Vulnerability - level 4	Practice
43375	Cisco IOS Software SSL VPN Denial of Service Vulnerability (cisco-sa-20140326-ios-sslvpn)	Potential Vulnerability - level 3	Practice
43376	Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20140326-sip)	Potential Vulnerability - level 3	Practice
43377	Cisco IOS Network Address Translation Denial of Service Vulnerabilities (cisco-sa-20140326-nat)	Potential Vulnerability - level 3	Practice
43378	Synology DiskStation Manager Multiple Vulnerabilities	Vulnerability - level 3	Vuln
43380	Cisco IOS Software Internet Key Exchange Version 2 Denial of Service Vulnerability (cisco-sa-20140326-ikev2)	Potential Vulnerability - level 3	Practice
43381	Cisco IOS Software Crafted IPv6 Packet Denial of Service Vulnerability (cisco-sa-20140326-ipv6)	Potential Vulnerability - level 3	Practice
43382	Ruggedcom ROS Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
43403	Cisco IOS Software IPsec Denial of Service Vulnerability (CSCui79745)	Potential Vulnerability - level 3	Practice
43416	Cisco IOS Software Metadata Vulnerabilities (cisco-sa-20140924-metadata)	Potential Vulnerability - level 4	Practice
43418	Cisco IOS Software DHCP Version 6 Denial of Service Vulnerability (cisco-sa-20140924-dhcpv6)	Potential Vulnerability - level 4	Practice
43419	Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20140924-sip)	Potential Vulnerability - level 4	Practice
43420	Cisco IOS Software Network Address Translation Denial of Service Vulnerability (cisco-sa-20140924-nat)	Potential Vulnerability - level 4	Practice
43421	Cisco IOS Software RSVP Vulnerability (cisco-sa-20140924-rsvp)	Vulnerability - level 4	Practice
43434	Cisco IOS Openssl Multiple Vulnerabilities (cisco-sa-20140605-openssl)	Vulnerability - level 4	Vuln
43435	Cisco IOS OpenSSL Multiple Vulnerabilities (cisco-sa-20150310-ssl)	Vulnerability - level 4	Vuln
43438	Cisco IOS Internet Key Exchange Version 2 Denial of Service Vulnerabilities (cisco-sa-20150325-ikev2)	Vulnerability - level 3	Vuln
43441	Cisco IOS TCP Packet Memory Leak Vulnerability (cisco-sa-20150325-tcpleak)	Vulnerability - level 3	Vuln
43463	Cisco NX-OS OpenSSL Multiple Vulnerabilities (cisco-sa-20151204-openssl)	Vulnerability - level 3	Vuln
43468	Cisco ASA OpenSSL Multiple Vulnerabilities (cisco-sa-20151204-openssl)	Vulnerability - level 3	Vuln
43476	Cisco NX-OS OpenSSL Multiple Vulnerabilities (cisco-sa-20160129-openssl)	Vulnerability - level 3	Vuln
43479	Cisco NX-OS Network Time Protocol Daemon Multiple Vulnerabilities (cisco-sa-20160127-ntpd)	Vulnerability - level 3	Vuln
43480	Cisco IOS Network Time Protocol Daemon Multiple Vulnerabilities (cisco-sa-20160127-ntpd)	Vulnerability - level 3	Vuln
43488	Cisco OpenSSL Multiple Vulnerabilities (cisco-sa-20160302-openssl)	Vulnerability - level 3	Vuln
43492	Cisco IOS Software Internet Key Exchange Version 2 Fragmentation Denial of Service Vulnerability (cisco-sa-20160323-ios-ikev2)	Vulnerability - level 4	Practice
43515	HPE ArubaOS Network Time Protocol Daemon (NTPD) Multiple Vulnerabilities (ARUBA-PSA-2015-010)	Vulnerability - level 4	Vuln
43516	HPE ArubaOS OpenSSL Multiple Vulnerabilities (ARUBA-PSA-2015-007)	Vulnerability - level 3	Vuln

43517	HPE ArubaOS Remote Access Point (RAP) Command Injection Vulnerability (ARUBA-PSA-2015-004)	Vulnerability - level 3	Vuln
43556	HPE A5120-48G-PoE+ EI Switch Remote Disclosure of Information Vulnerability	Vulnerability - level 3	Vuln
43559	HPE ArubaOS WPA2 Key Reinstallation (KRACKs Attack) Vulnerabilities (ARUBA-PSA-2017-007)	Vulnerability - level 3	Vuln
43578	HPE Integrated Lights-Out 2 (iLO 2) Remote Disclosure of Information Vulnerability	Vulnerability - level 3	Vuln
43582	Juniper JUNOS Stunnel Multiple Vulnerabilities (JSA10852)	Vulnerability - level 3	Vuln
43588	Huawei Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (huawei-sa-20160706-01-openssl)	Vulnerability - level 5	Vuln
43589	Huawei Products Bar Mitzvah Attack Vulnerability(hw-454055)	Vulnerability - level 3	Vuln
43596	Huawei NIP5100 SNMP Vulnerability(hw-197483)	Vulnerability - level 3	Vuln
43608	Juniper JUNOS SegmentSmack Vulnerability (JSA10876)	Potential Vulnerability - level 3	Practice
43619	Juniper Junos OS Multiple vulnerabilities in cURL versions (JSA10874)	Vulnerability - level 4	Vuln
43651	Juniper Network Operating System (Junos OS) Open Secure Sockets Layer (OpenSSL) Multiple Security Vulnerabilities (JSA10919)	Vulnerability - level 4	Vuln
43656	Fortigate FortiOS Information Disclosure, Privilege Escalation Vulnerability (FG-IR-18-002)	Vulnerability - level 3	Vuln
43669	Arista EOS Authentication vulnerability (SA0036)	Vulnerability - level 3	Vuln
43694	Juniper Junos OpenSSH Multiple Vulnerabilities (JSA10940)	Vulnerability - level 3	Vuln
43771	A10 Networks Advanced Core Operating System (ACOS) Security Updates for Secure Sockets Layer (SSL) (ssl-cve-2019-1563)	Vulnerability - level 2	Vuln
43772	A10 Networks ACOS Security Updates for HTTP/2 (http-2-multiple-dos-vulnerabilities)	Vulnerability - level 2	Vuln
43775	A10 Networks Advanced Core Operating System (ACOS) Security Updates for Transport Layer Security (TLS)/Secure Sockets Layer (SSL) (tls-ssl-cve-2016-2177)	Vulnerability - level 5	Vuln
43781	A10 Networks ACOS Security Updates for TCP/IP (tcp-ip-cve-2018-5390-segmentsmack)	Vulnerability - level 4	Vuln
43783	A10 Networks Advanced Core Operating System (ACOS) Security Updates for Transport Layer Security (TLS)/Secure Sockets Layer (SSL) (tls-ssl-cve-2016-2182/)	Vulnerability - level 5	Vuln
43785	A10 Networks Advanced Core Operating System (ACOS) Security Updates for Transport Layer Security (TLS)/Secure Sockets Layer (SSL) (tls-ssl-cve-2016-6306)	Vulnerability - level 3	Vuln
43787	A10 Networks Advanced Core Operating System (ACOS) Security Updates for Transport Layer Security (TLS)/Secure Sockets Layer (SSL) (tls-ssl-cve-2016-6302)	Vulnerability - level 4	Vuln
43790	A10 Networks Advanced Core Operating System (ACOS) Security Updates for Transport Layer Security (TLS)/Secure Sockets Layer (SSL) (tls-ssl-cve-2018-0732)	Vulnerability - level 3	Vuln
43791	A10 Networks Advanced Core Operating System (ACOS) Security Updates for Transport Layer Security (TLS)/Secure Sockets Layer (SSL) (tls-ssl-cve-2017-3735)	Vulnerability - level 3	Vuln
43792	A10 Networks Advanced Core Operating System (ACOS) Security Updates for Transport Layer Security (TLS)/Secure Sockets Layer (SSL) (tls-ssl-cve-2017-3736-3737-3738)	Vulnerability - level 3	Vuln
43796	A10 Networks ACOS Security Updates for SSH DH MODULUS (ssh-dh-modulus-1024-bits-logjam)	Vulnerability - level 3	Vuln
43804	A10 Networks ACOS Security Updates for SYSTEM (system-vulnerabilities-1-acos-3-x-4-x)	Vulnerability - level 5	Vuln
43808	A10 Networks ACOS Security Updates for NTP (ntp-cve-2016-7429-cve-2016-7433)	Vulnerability - level 3	Vuln
43828	Hewlett Packard Enterprise (HPE) ArubaOS Multiple Vulnerabilities (ARUBA-PSA-2021-011)	Vulnerability - level 3	Vuln

43856	Hewlett Packard Enterprise (HPE) ArubaOS SAD Domain Name System (DNS) Side Channel Vulnerability (ARUBA-PSA-2021-008)	Vulnerability - level 3	Vuln
43857	Hewlett Packard Enterprise (HPE) ArubaOS Buffer Overflow Vulnerability (ARUBA-PSA-2021-016)	Vulnerability - level 4	Vuln
43860	Hewlett Packard Enterprise (HPE) ArubaOS Remote Command Execution Vulnerability (ARUBA-PSA-2021-016)	Vulnerability - level 4	Vuln
43861	Hewlett Packard Enterprise (HPE) ArubaOS Remote Command Execution Vulnerability (ARUBA-PSA-2021-016)	Vulnerability - level 4	Vuln
43862	Hewlett Packard Enterprise (HPE) ArubaOS Remote Command Execution Vulnerability (ARUBA-PSA-2021-016)	Vulnerability - level 4	Vuln
43863	Hewlett Packard Enterprise (HPE) ArubaOS Cross-Site Request Forgery (CSRF) Vulnerability (ARUBA-PSA-2021-016)	Vulnerability - level 3	Vuln
43864	Hewlett Packard Enterprise (HPE) ArubaOS Cross-Site Request Forgery (CSRF) Vulnerability (ARUBA-PSA-2021-016)	Potential Vulnerability - level 2	Practice
43865	Hewlett Packard Enterprise (HPE) ArubaOS Local Path Traversal Vulnerability (ARUBA-PSA-2021-016)	Vulnerability - level 3	Vuln
43866	Hewlett Packard Enterprise (HPE) ArubaOS Denial of Service (DoS) Vulnerability (ARUBA-PSA-2021-016)	Vulnerability - level 3	Vuln
43867	Hewlett Packard Enterprise (HPE) ArubaOS Denial of Service (DoS) Vulnerability (ARUBA-PSA-2021-016)	Vulnerability - level 3	Vuln
43884	Huawei Router Side-channel Central Processing Unit (CPU) hardware Vulnerability (Huawei-SA-20180615-01-cpu-en)	Vulnerability - level 2	Vuln
43894	Cisco IOS Software Session Initiation Protocol Memory Leak Vulnerability (cisco-sa-20160323-sip)	Vulnerability - level 4	Practice
43988	Hewlett Packard Enterprise (HPE) ArubaOS Multiple Vulnerabilities (ARUBA-PSA-2023-002)	Potential Vulnerability - level 4	Practice
44025	Juniper Network Operating System (Junos OS) Multiple Vulnerabilities (JSA70605)	Potential Vulnerability - level 4	Practice
44030	Juniper Network Operating System (Junos OS) Multiple NTP Vulnerabilities (JSA11171)	Potential Vulnerability - level 4	Practice
500021	Alpine Linux Security Update for apache2	Vulnerability - level 5	Vuln
500022	Alpine Linux Security Update for apache2	Vulnerability - level 5	Vuln
500026	Alpine Linux Security Update for apache2	Vulnerability - level 5	Vuln
500059	Alpine Linux Security Update for bind	Vulnerability - level 4	Vuln
500060	Alpine Linux Security Update for bind	Vulnerability - level 5	Vuln
500062	Alpine Linux Security Update for bind	Vulnerability - level 4	Vuln
500082	Alpine Linux Security Update for busybox	Vulnerability - level 4	Vuln
500110	Alpine Linux Security Update for curl	Vulnerability - level 4	Vuln
500111	Alpine Linux Security Update for curl	Vulnerability - level 4	Vuln
500113	Alpine Linux Security Update for curl	Vulnerability - level 5	Vuln
500114	Alpine Linux Security Update for curl	Vulnerability - level 5	Vuln
500125	Alpine Linux Security Update for curl	Vulnerability - level 5	Vuln
500126	Alpine Linux Security Update for curl	Vulnerability - level 5	Vuln
500133	Alpine Linux Security Update for curl	Vulnerability - level 2	Vuln
500150	Alpine Linux Security Update for dnsmasq	Vulnerability - level 4	Vuln
500174	Alpine Linux Security Update for elfutils	Vulnerability - level 4	Vuln
500177	Alpine Linux Security Update for expat	Vulnerability - level 5	Vuln
500178	Alpine Linux Security Update for expat	Vulnerability - level 5	Vuln
500179	Alpine Linux Security Update for expat	Vulnerability - level 5	Vuln
500246	Alpine Linux Security Update for hostapd	Vulnerability - level 4	Vuln
500289	Alpine Linux Security Update for libexif	Vulnerability - level 4	Vuln
500324	Alpine Linux Security Update for libuv	Vulnerability - level 4	Vuln
500340	Alpine Linux Security Update for libxml2	Vulnerability - level 4	Vuln
500342	Alpine Linux Security Update for libxml2	Vulnerability - level 4	Vuln
500343	Alpine Linux Security Update for libxml2	Vulnerability - level 3	Vuln
500344	Alpine Linux Security Update for libxml2	Vulnerability - level 4	Vuln
500350	Alpine Linux Security Update for libxml2	Vulnerability - level 4	Vuln
500368	Alpine Linux Security Update for libressl	Vulnerability - level 4	Vuln
500424	Alpine Linux Security Update for nghttp2	Vulnerability - level 4	Vuln

500436	Alpine Linux Security Update for nodejs	Vulnerability - level 4	Vuln
500437	Alpine Linux Security Update for nodejs	Vulnerability - level 4	Vuln
500439	Alpine Linux Security Update for nodejs	Vulnerability - level 4	Vuln
500443	Alpine Linux Security Update for nodejs	Vulnerability - level 5	Vuln
500445	Alpine Linux Security Update for nodejs	Vulnerability - level 4	Vuln
500454	Alpine Linux Security Update for nss	Vulnerability - level 3	Vuln
500455	Alpine Linux Security Update for nss	Vulnerability - level 4	Vuln
500480	Alpine Linux Security Update for openldap	Vulnerability - level 4	Vuln
500484	Alpine Linux Security Update for openssh	Vulnerability - level 4	Vuln
500485	Alpine Linux Security Update for openssh	Vulnerability - level 3	Vuln
500493	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 3	Vuln
500496	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 3	Vuln
500497	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 4	Vuln
500498	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 4	Vuln
500499	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 5	Vuln
500502	Alpine Linux Security Update for Open Virtual Private Network (OpenVPN)	Vulnerability - level 5	Vuln
500542	Alpine Linux Security Update for postgresql	Vulnerability - level 4	Vuln
500561	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 3	Vuln
500564	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 3	Vuln
500565	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 4	Vuln
500566	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 4	Vuln
500567	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 5	Vuln
500570	Alpine Linux Security Update for Open Virtual Private Network (OpenVPN)	Vulnerability - level 5	Vuln
500585	Alpine Linux Security Update for python2	Vulnerability - level 5	Vuln
500652	Alpine Linux Security Update for sqlite	Vulnerability - level 4	Vuln
500671	Alpine Linux Security Update for subversion	Vulnerability - level 4	Vuln
500692	Alpine Linux Security Update for tiff	Vulnerability - level 3	Vuln
500739	Alpine Linux Security Update for wpa_supplicant	Vulnerability - level 3	Vuln
500740	Alpine Linux Security Update for wpa_supplicant	Vulnerability - level 4	Vuln
500789	Alpine Linux Security Update for xen	Vulnerability - level 3	Vuln
501057	Alpine Linux Security Update for libreswan	Vulnerability - level 4	Vuln
501067	Alpine Linux Security Update for libvncserver	Vulnerability - level 4	Vuln
501068	Alpine Linux Security Update for libvncserver	Vulnerability - level 4	Vuln
501072	Alpine Linux Security Update for lldpd	Vulnerability - level 4	Vuln
501097	Alpine Linux Security Update for nodejs-current	Vulnerability - level 4	Vuln
501192	Alpine Linux Security Update for intel-ucode	Vulnerability - level 3	Vuln
501193	Alpine Linux Security Update for intel-ucode	Vulnerability - level 3	Vuln
501194	Alpine Linux Security Update for intel-ucode	Vulnerability - level 3	Vuln
501195	Alpine Linux Security Update for intel-ucode	Vulnerability - level 4	Vuln
501353	Alpine Linux Security Update for apache2	Vulnerability - level 4	Vuln
501382	Alpine Linux Security Update for bind	Vulnerability - level 3	Vuln
501383	Alpine Linux Security Update for bind	Vulnerability - level 4	Vuln
501387	Alpine Linux Security Update for busybox	Vulnerability - level 4	Vuln
501396	Alpine Linux Security Update for curl	Vulnerability - level 4	Vuln
501400	Alpine Linux Security Update for expat	Vulnerability - level 5	Vuln
501401	Alpine Linux Security Update for expat	Vulnerability - level 5	Vuln
501402	Alpine Linux Security Update for expat	Vulnerability - level 5	Vuln

501420	Alpine Linux Security Update for libressl	Vulnerability - level 3	Vuln
501421	Alpine Linux Security Update for libuv	Vulnerability - level 4	Vuln
501423	Alpine Linux Security Update for libxml2	Vulnerability - level 4	Vuln
501424	Alpine Linux Security Update for libxml2	Vulnerability - level 3	Vuln
501444	Alpine Linux Security Update for nodejs	Vulnerability - level 4	Vuln
501448	Alpine Linux Security Update for nodejs	Vulnerability - level 4	Vuln
501452	Alpine Linux Security Update for nodejs	Vulnerability - level 5	Vuln
501454	Alpine Linux Security Update for nodejs	Vulnerability - level 4	Vuln
501458	Alpine Linux Security Update for openldap	Vulnerability - level 4	Vuln
501459	Alpine Linux Security Update for openldap	Vulnerability - level 4	Vuln
501467	Alpine Linux Security Update for Open Virtual Private Network (OpenVPN)	Vulnerability - level 5	Vuln
501470	Alpine Linux Security Update for postgresql	Vulnerability - level 4	Vuln
501487	Alpine Linux Security Update for rssh	Vulnerability - level 5	Vuln
501488	Alpine Linux Security Update for rssh	Vulnerability - level 5	Vuln
501509	Alpine Linux Security Update for xen	Vulnerability - level 3	Vuln
501572	Alpine Linux Security Update for go	Vulnerability - level 3	Vuln
501636	Alpine Linux Security Update for nodejs-current	Vulnerability - level 4	Vuln
501637	Alpine Linux Security Update for nodejs-current	Vulnerability - level 4	Vuln
501655	Alpine Linux Security Update for openvswitch	Vulnerability - level 5	Vuln
501694	Alpine Linux Security Update for synapse	Vulnerability - level 3	Vuln
501734	Alpine Linux Security Update for busybox	Vulnerability - level 3	Vuln
501735	Alpine Linux Security Update for busybox	Vulnerability - level 4	Vuln
501738	Alpine Linux Security Update for expat	Vulnerability - level 5	Vuln
501739	Alpine Linux Security Update for expat	Vulnerability - level 5	Vuln
501740	Alpine Linux Security Update for expat	Vulnerability - level 5	Vuln
501748	Alpine Linux Security Update for libxml2	Vulnerability - level 4	Vuln
501829	Alpine Linux Security Update for containerd	Vulnerability - level 4	Vuln
501837	Alpine Linux Security Update for docker	Vulnerability - level 4	Vuln
501855	Alpine Linux Security Update for go	Vulnerability - level 4	Vuln
501856	Alpine Linux Security Update for go	Vulnerability - level 5	Vuln
501861	Alpine Linux Security Update for go	Vulnerability - level 3	Vuln
501862	Alpine Linux Security Update for go	Vulnerability - level 4	Vuln
501883	Alpine Linux Security Update for newlib	Vulnerability - level 5	Vuln
501885	Alpine Linux Security Update for nodejs-current	Vulnerability - level 5	Vuln
501915	Alpine Linux Security Update for qt5-qtwebengine	Vulnerability - level 4	Vuln
501948	Alpine Linux Security Update for bind	Vulnerability - level 3	Vuln
501950	Alpine Linux Security Update for busybox	Vulnerability - level 4	Vuln
501968	Alpine Linux Security Update for libxml2	Vulnerability - level 4	Vuln
501979	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)	Vulnerability - level 3	Vuln
501982	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)	Vulnerability - level 3	Vuln
501983	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)	Vulnerability - level 4	Vuln
501984	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)	Vulnerability - level 4	Vuln
501985	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)	Vulnerability - level 5	Vuln
501987	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)	Vulnerability - level 5	Vuln
501993	Alpine Linux Security Update for postgresql13	Vulnerability - level 4	Vuln
502010	Alpine Linux Security Update for postgresql14	Vulnerability - level 4	Vuln
502090	Alpine Linux Security Update for go	Vulnerability - level 4	Vuln
502092	Alpine Linux Security Update for go	Vulnerability - level 4	Vuln
502093	Alpine Linux Security Update for go	Vulnerability - level 5	Vuln
502126	Alpine Linux Security Update for nomad	Vulnerability - level 4	Vuln
502179	Alpine Linux Security Update for qt5-qtwebengine	Vulnerability - level 5	Vuln
502297	Alpine Linux Security Update for go	Vulnerability - level 4	Vuln

502299	Alpine Linux Security Update for go	Vulnerability - level 4	Vuln
502300	Alpine Linux Security Update for go	Vulnerability - level 4	Vuln
502316	Alpine Linux Security Update for nomad	Vulnerability - level 4	Vuln
502358	Alpine Linux Security Update for qt5-qtwebengine	Vulnerability - level 5	Vuln
502387	Alpine Linux Security Update for thunderbird	Vulnerability - level 4	Vuln
502413	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 4	Vuln
502415	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)	Vulnerability - level 4	Vuln
502416	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)	Vulnerability - level 4	Vuln
502445	Alpine Linux Security Update for nodejs	Vulnerability - level 4	Vuln
502446	Alpine Linux Security Update for nodejs	Vulnerability - level 4	Vuln
502447	Alpine Linux Security Update for nodejs-current	Vulnerability - level 4	Vuln
502486	Alpine Linux Security Update for libxml2	Vulnerability - level 4	Vuln
502513	Alpine Linux Security Update for nodejs-current	Vulnerability - level 5	Vuln
502514	Alpine Linux Security Update for nodejs-current	Vulnerability - level 5	Vuln
502652	Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)	Vulnerability - level 4	Vuln
502653	Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)	Vulnerability - level 4	Vuln
502674	Alpine Linux Security Update for e2fsprogs	Vulnerability - level 4	Vuln
502730	Alpine Linux Security Update for grub	Vulnerability - level 4	Vuln
502752	Alpine Linux Security Update for openssl	Vulnerability - level 4	Vuln
502753	Alpine Linux Security Update for openssl	Vulnerability - level 3	Vuln
502757	Alpine Linux Security Update for openssl	Vulnerability - level 4	Vuln
502776	Alpine Linux Security Update for postgresql15	Vulnerability - level 4	Vuln
502898	Alpine Linux Security Update for openssl1.1-compatible	Vulnerability - level 3	Vuln
502901	Alpine Linux Security Update for openssl1.1-compatible	Vulnerability - level 3	Vuln
502902	Alpine Linux Security Update for openssl1.1-compatible	Vulnerability - level 4	Vuln
502903	Alpine Linux Security Update for openssl1.1-compatible	Vulnerability - level 4	Vuln
502904	Alpine Linux Security Update for openssl1.1-compatible	Vulnerability - level 5	Vuln
502906	Alpine Linux Security Update for openssl1.1-compatible	Vulnerability - level 3	Vuln
502907	Alpine Linux Security Update for openssl1.1-compatible	Vulnerability - level 4	Vuln
502932	Alpine Linux Security Update for qt5-qtwebengine	Vulnerability - level 4	Vuln
502980	Alpine Linux Security Update for e2fsprogs	Vulnerability - level 4	Vuln
520011	Open Secure Sockets Layer (OpenSSL) Type Confusion Vulnerability (CVE-2023-0286)	Potential Vulnerability - level 4	Practice
53001	Microsoft Exchange Server Information Disclosure Vulnerabilities (MS15-103)	Vulnerability - level 3	Vuln
590006	Siemens Automation License Manager 5.x(prior to 5.3.4.4) Multiple Vulnerabilities (ICSA-18-226-03)	Vulnerability - level 3	Vuln
590007	Siemens Automation License Manager Vulnerabilities(ICSA-16-287-02)	Vulnerability - level 3	Vuln
590008	Rockwell Automation FactoryTalk Diagnostics Deserialization of Untrusted Data vulnerability (ICSA-20-051-02)	Vulnerability - level 3	Vuln
590009	Rockwell Automation RSLinx ClassicStack-based Buffer Overflow Vulnerability (ICSA-19-064-01)	Vulnerability - level 3	Vuln
590010	Siemens SIMATIC STEP 7 (TIA Portal) Unprotected Storage of Credentials Vulnerability (ICSA-18-317-06)	Vulnerability - level 2	Vuln
590011	Siemens SIMATIC STEP 7 (TIA Portal)and SIMATIC WinCC (TIA Portal) Incorrect Default Permissions Vulnerability (ICSA-18-226-01)	Vulnerability - level 3	Vuln
590012	Siemens WinCC TIA Portal Multiple Vulnerabilities (ICSA-13-079-03)	Vulnerability - level 3	Vuln
590013	Siemens WinCC TIA Portal Vulnerabilities (ICSA-13-213-02)	Vulnerability - level 3	Vuln
590014	Siemens SIMATIC WinCC TIA Portal Vulnerabilities (ICSA-15-048-02)	Vulnerability - level 3	Vuln

590015	Siemens SIMATIC WinCC Multiple Vulnerabilities (ICSA-12-030-01A)	Vulnerability - level 5	Vuln
590016	Siemens WinCC Flexible Runtime Heap Overflow Vulnerability (ICSA-11-244-01)	Vulnerability - level 4	Vuln
590017	Siemens SIMATIC PCS 7 Improper Input Validation Vulnerability (ICSA-17-306-01)	Vulnerability - level 3	Vuln
590018	Siemens WinCC WebNavigator Multiple Vulnerabilities (ICSA-12-256-01)	Vulnerability - level 3	Vuln
590020	Rockwell Automation FactoryTalk and RSLinx Multiple Vulnerabilities (ICSA-13-095-02A)	Vulnerability - level 5	Vuln
590021	Rockwell Automation RSLinx Classic vulnerability(ICSA-18-263-02)	Vulnerability - level 3	Vuln
590023	Siemens WinCC 7.0 SP3 Multiple Vulnerabilities (ICSA-13-079-02)	Vulnerability - level 3	Vuln
590024	Rockwell Automation FactoryTalk RNADiagReceiver Multiple Vulnerabilities(ICSA-12-088-01A)	Vulnerability - level 3	Vuln
590025	Siemens SIMATIC WinCC Multiple Vulnerabilities (Update A) (ICSA-14-205-02A)	Vulnerability - level 3	Vuln
590027	Rockwell Automation FactoryTalk Activation Manager (Update B) (ICSA-18-102-02)	Vulnerability - level 4	Vuln
590028	Siemens SIMATIC NET PC-Software Denial-of-Service Vulnerability (ICSA-16-208-02)	Vulnerability - level 3	Vuln
590029	Rockwell Automation FactoryTalk Services Platform DoS Vulnerability (ICSA-18-331-02)	Vulnerability - level 3	Vuln
590030	Rockwell Automation FactoryTalk Alarms and Events DoS Vulnerability (ICSA-17-341-02)	Vulnerability - level 3	Vuln
590031	Rockwell Automation Connected Components Workbench DLL Hijack Vulnerability (ICSA-17-047-01)	Vulnerability - level 3	Vuln
590032	Siemens SIMATIC Logon Authentication Bypass Vulnerability (ICSA-17-045-03)	Vulnerability - level 3	Vuln
590033	Rockwell RSLogix 5000 Password Vulnerability (ICSA-14-021-01)	Vulnerability - level 3	Vuln
590034	Rockwell Automation Arena DoS Vulnerability (ICSA-18-130-02)	Vulnerability - level 3	Vuln
590035	Rockwell Automation FactoryTalk DLL Hijacking Vulnerability (ICSA-15-062-02)	Vulnerability - level 3	Vuln
590036	Rockwell Automation Arena Simulation Software (Update B) Multiple Vulnerabilities(icsa-19-213-05)	Vulnerability - level 3	Vuln
590037	Rockwell Automation EDS Subsystem Multiple Vulnerabilities(ICSA-20-140-01)	Vulnerability - level 3	Vuln
590038	Rockwell Automation RSLinx Classic Vulnerability(ICSA-20-100-01)	Vulnerability - level 3	Vuln
590039	Siemens LOGO! Soft Comfort Vulnerability(ICSA-17-353-04)	Vulnerability - level 3	Vuln
590040	Rockwell Automation RSView32 Weak Encryption Algorithm on Passwords Vulnerability(ICSA-15-132-02)	Vulnerability - level 3	Vuln
590041	Rockwell Automation RSLogix 500 Software Multiple Vulnerabilities(ICSA-20-070-06)	Vulnerability - level 5	Vuln
590043	Rockwell Automation RSLinx Classic Vulnerability Vulnerability(ICSA-15-111-02)	Vulnerability - level 3	Vuln
590045	Rockwell Automation FactoryTalk Activation Vulnerability(ICSA-17-047-02)	Vulnerability - level 3	Vuln
590049	Siemens SIMATIC WinCC OA Vulnerability(ICSA-18-254-04)	Vulnerability - level 3	Vuln
590050	OSIsoft PI Vision Multiple Vulnerabilities(ICSA-20-014-06)	Vulnerability - level 3	Vuln
590051	OSIsoft PI Vision Multiple Cross Site Scripting Vulnerability (ICSA-20-014-06)	Vulnerability - level 3	Vuln
590052	OSIsoft PI Vision sensitive information discolsure Vulnerability(ICSA-20-014-06)	Vulnerability - level 2	Vuln
590053	Siemens SICAM PAS Vulnerabilities (Update A) Multiple Vulnerabilities(ICSA-16-336-01)	Vulnerability - level 3	Vuln
590054	Rockwell Automation Integrated Architecture Builder Access Violation Memory Error Vulnerability(ICSA-16-056-01)	Vulnerability - level 3	Vuln

590055	Rockwell FactoryTalk View sensitive information disclosure Vulnerability(ICS-20-177-03)	Vulnerability - level 3	Vuln
590056	Rockwell FactoryTalk View SE Weak Encryption Algorithm on Passwords Vulnerability(ICS-20-177-03)	Vulnerability - level 3	Vuln
590058	Rockwell FactoryTalk Services Platform XXE Vulnerability(ICS-20-177-02)	Vulnerability - level 3	Vuln
590059	Rockwell Automation FactoryTalk View SE Client configuration parsing error vulnerability(ICS-20-170-05)	Vulnerability - level 3	Vuln
590060	Siemens IEC 61850 System Configurator, DIGSI 5, DIGSI 4, SICAM PAS/PQS, and SICAM SCC Vulnerability(ICS-18-317-01)	Vulnerability - level 5	Vuln
590061	Siemens TIA Portal Local Privilege Escalation Vulnerability Vulnerability(ICS-20-014-05)	Potential Vulnerability - level 3	Practice
590062	Rockwell Automation FactoryTalk Linx Software (Update A) Multiple Vulnerabilities(ICS-20-163-02)	Vulnerability - level 3	Vuln
590063	Rockwell Automation Logix Designer Studio 5000 Vulnerability(ICS-20-191-02)	Vulnerability - level 3	Vuln
590064	Siemens SIMATIC Products (Update B) man-in-the-middle attack Vulnerability(ICS-19-344-04)	Vulnerability - level 3	Vuln
590066	Siemens SIMATIC Panels and SIMATIC WinCC (TIA Portal) HTTP Header Injection Vulnerability (ICS-18-317-03)	Vulnerability - level 3	Vuln
590067	Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC Denial-of-Service Vulnerability(ICS-20-042-06)	Vulnerability - level 3	Vuln
590068	Siemens WinCC (TIA Portal) Multiple Vulnerabilities(ICS-19-134-09)	Vulnerability - level 3	Vuln
590069	Siemens SIMATIC WinCC and PCS7 (Update C) Code Upload Vulnerability (ICS-19-192-02)	Vulnerability - level 3	Vuln
590070	Schneider Electric Software Update (SEU) DLL hijacking vulnerability(ICS-18-305-02)	Vulnerability - level 4	Vuln
590071	Schneider Electric Ampla MES Multiple Vulnerabilities(ICS-17-187-05)	Vulnerability - level 2	Vuln
590072	Schneider Electric Wonderware Historian Client XXE Vulnerability(ICS-17-122-01)	Vulnerability - level 3	Vuln
590073	Schneider Electric Wonderware InTouch Access Anywhere Multiple Vulnerabilities(ICS-17-089-01)	Vulnerability - level 3	Vuln
590074	Schneider Electric Unity PRO Control Flow Management Vulnerability Vulnerability(ICS-16-306-03)	Vulnerability - level 3	Vuln
590075	Siemens SIMATIC PCS7, WinCC, TIA Portal (Update D) Multiple Vulnerabilities(ICS-19-134-08)	Vulnerability - level 5	Vuln
590076	Schneider Electric Pro-face GP-Pro EX Vulnerability(ICS-19-003-01)	Vulnerability - level 3	Vuln
590077	Schneider Electric Pro-face GP-Pro EX DLL/OCX file Vulnerability(ICS-17-215-01)	Vulnerability - level 3	Vuln
590079	Siemens Industrial Products Local Privilege Escalation Vulnerability (Update I) Vulnerability(ICS-16-313-02)	Vulnerability - level 3	Vuln
590080	Siemens Automation License Manager Local Privilege Escalation Vulnerability(ICS-20-224-07)	Potential Vulnerability - level 3	Practice
590081	Siemens OPC UA Protocol Stack Discovery Service (Update D) XXE Vulnerability (ICS-17-243-01-0)	Vulnerability - level 3	Vuln
590082	Siemens LOGO! Soft Comfort Code Execution Vulnerability(ICS-19-134-03)	Vulnerability - level 3	Vuln
590083	Siemens SIMATIC WinCC and SIMATIC PCS 7 Remote Code Execution Vulnerability(ICS-19-134-02-0)	Vulnerability - level 3	Vuln
590084	Siemens SIMATIC, SINAMICS (Update A) Multiple Vulnerabilities(ICS-20-161-05)	Vulnerability - level 3	Vuln
590085	Siemens Industrial Products with OPC UA (Update F) DoS Vulnerability(ICS-19-099-03)	Vulnerability - level 3	Vuln
590086	Siemens SIMATIC HMI Panels Clear Text Transmission Vulnerability(ICS-20-196-04)	Vulnerability - level 3	Vuln

590087	Siemens TD Keypad Designer Local Privilege Escalation Vulnerability(ICS-18-254-03)	Vulnerability - level 5	Vuln
590088	Siemens Open Secure Sockets Layer (OpenSSL) Vulnerability in Industrial Products (Update E) Vulnerability (ICSA-18-226-02)	Vulnerability - level 3	Vuln
590089	Siemens SIMATIC WinCC and SIMATIC PCS 7 ActiveX Vulnerability(ICSA-16-348-04)	Vulnerability - level 3	Vuln
590090	Siemens DIGSI 4 Multiple Vulnerabilities(ICSA-18-067-01)	Vulnerability - level 3	Vuln
590091	Siemens SIMATIC Logon Denial of Service Vulnerability (ICSA-17-192-01)	Vulnerability - level 3	Vuln
590092	Siemens SICAM PAS Information Disclosure Vulnerabilities(ICSA-16-182-02)	Vulnerability - level 2	Vuln
590093	Siemens devices using the PROFINET Discovery and Configuration Protocol Denial-of-Service Vulnerability (ICSA-17-129-01)	Vulnerability - level 3	Vuln
590095	Siemens WinCC 7.2 Multiple Vulnerabilities(ICSA-13-169-02)	Vulnerability - level 3	Vuln
590097	Mitsubishi Electric Factory Automation Products Path Traversal Vulnerability(ICSA-20-212-03)	Vulnerability - level 3	Vuln
590098	Advantech WebAccess HMI Designer Multiple Vulnerabilities(ICSA-20-219-02)	Vulnerability - level 3	Vuln
590099	Siemens SINEMA Server Privilege Escalation Vulnerability (Update A) Vulnerability(ICSA-16-215-02)	Vulnerability - level 3	Vuln
590100	Advantech iView Vulnerability(ICSA-20-238-01)	Vulnerability - level 3	Vuln
590101	Siemens SIMATIC STEP 7 TIA Portal Multiple Vulnerabilities(ICSA-15-048-01)	Vulnerability - level 3	Vuln
590102	Siemens SIMATIC WinCC and SIMATIC WinCC Runtime Professional Vulnerability(ICSA-17-129-03)	Vulnerability - level 3	Vuln
590103	Siemens SIMATIC STEP 7 TIA Portal (Update A) Multiple Vulnerabilities(ICSA-15-050-01A)	Vulnerability - level 3	Vuln
590104	Siemens SIMATIC WinCC, PCS 7, and WinCC Runtime Professional (Update C) Multiple Vulnerabilities(ICSA-16-208-01)	Vulnerability - level 5	Vuln
590105	Siemens SIMATIC WinCC Flexible Weakly Protected Credentials Vulnerability(ICSA-16-161-02)	Vulnerability - level 3	Vuln
590106	Schneider Electric Zelio Soft 2 Vulnerability(ICSA-19-008-01)	Vulnerability - level 3	Vuln
590107	Schneider Electric InduSoft Web Studio and InTouch Machine Edition Vulnerability(ICSA-18-107-01)	Vulnerability - level 3	Vuln
590108	Siemens SIMATIC PCS 7, SIMATIC WinCC, SIMATIC WinCC Runtime Professional, and SIMATIC NET PC Software (Update G) Vulnerability(ICSA-18-088-03)	Potential Vulnerability - level 3	Practice
590111	Siemens WinCC Multiple Vulnerabilities(ICSA-12-158-01)	Vulnerability - level 3	Vuln
590112	Schneider Electric EcoStruxure Operator Terminal Expert Multiple Vulnerabilities(SEVD-2020-133-04)	Vulnerability - level 3	Vuln
590113	Mitsubishi Electric Multiple Factory Automation Engineering Software Products Vulnerability(ICSA-20-212-02)	Vulnerability - level 3	Vuln
590114	Rockwell Automation FactoryTalk Services Platform Vulnerability(ICSA-20-170-04)	Potential Vulnerability - level 3	Practice
590115	Siemens Automation License Manager Uncontrolled Resource Consumption Vulnerability(ICSA-12-349-01)	Vulnerability - level 3	Vuln
590116	AVEVA Vijeo Citect and Citect SCADA Vulnerability(ICSA-18-331-01)	Vulnerability - level 5	Vuln
590120	OSIsoft PI Data Archive Multiple Vulnerabilities(ICSA-18-072-02)	Vulnerability - level 3	Vuln
590121	Rockwell Automation FactoryTalk EnergyMetrix Multiple Vulnerabilities(ICSA-16-173-03)	Vulnerability - level 3	Vuln
590124	Mitsubishi Electric Factory Automation Engineering Products (Update A) Vulnerability(ICSA-20-212-04)	Vulnerability - level 3	Vuln
590126	OSIsoft PI Coresight Vulnerability(ICSA-17-192-04)	Vulnerability - level 3	Vuln
590127	AVEVA Vijeo Citect and Citect SCADA Floating License Manager Multiple Vulnerabilities(ICSA-19-192-05,ICSA-19-192-07)	Vulnerability - level 3	Vuln
590128	OSIsoft PI Vision Multiple Vulnerabilities(ICSA-18-072-03)	Vulnerability - level 3	Vuln

590131	Schneider Electric PowerSCADA Anywhere and Citect Anywhere Multiple Vulnerabilities(ICSA-17-201-01)	Vulnerability - level 3	Vuln
590132	OSIsoft PI Web API 2015 R2 Service Account Permissions Vulnerability Vulnerability(ICSA-16-287-01)	Vulnerability - level 3	Vuln
590133	OSIsoft PI Web API Multiple Vulnerabilities(ICSA-18-072-04)	Vulnerability - level 3	Vuln
590134	OSIsoft PI Web API 2017 Vulnerability(ICSA-17-164-03)	Potential Vulnerability - level 3	Practice
590135	GE CIMPLICITY (Update A) Stack-based Buffer Overflow Vulnerability(ICSA-17-278-01A)	Vulnerability - level 3	Vuln
590136	OSIsoft PI Server 2017 Multiple Vulnerabilities(ICSA-17-164-02)	Vulnerability - level 3	Vuln
590138	AVEVA Vijeo Citect and CitectSCADA Vulnerability(ICSA-19-150-01)	Vulnerability - level 2	Vuln
590139	GE Communicator buffer overflow Vulnerability(ICSA-18-275-02)	Vulnerability - level 3	Vuln
590140	GE Proficy HMI/SCADA iFIX, Proficy HMI/SCADA CIMPLICITY, and Proficy Historian Vulnerability (Update B) Vulnerability(ICSA-16-336-05B)	Vulnerability - level 3	Vuln
590141	AVEVA InduSoft Web Studio and InTouch Edge HMI Vulnerability(ICSA-19-078-01,ICSA-19-036-01)	Vulnerability - level 5	Vuln
590142	Schneider Electric Wonderware InduSoft Web Studio Vulnerability(ICSA-17-138-02)	Vulnerability - level 3	Vuln
590143	AVEVA Vijeo Citect and Citect SCADA (Update A) Vulnerability(ICSA-19-290-01)	Vulnerability - level 3	Vuln
590144	Rockwell Automation FactoryTalk Linx Multiple Vulnerabilities(ICSA-20-329-01)	Vulnerability - level 3	Vuln
590145	GE Proficy HMI/SCADA CIMPLICITY CimView Memory Access Violation Vulnerability(ICSA-14-289-02)	Vulnerability - level 3	Vuln
590146	Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 (Update A) Multiple Vulnerabilities(ICSA-15-085-01A)	Vulnerability - level 3	Vuln
590147	Schneider Electric IGSS SCADA Software Vulnerability(ICSA-18-044-02)	Vulnerability - level 3	Vuln
590148	Schneider Electric Zelio Soft 2 Vulnerability(ICSA-19-190-03)	Vulnerability - level 3	Vuln
590149	GE Proficy HMI SCADA CIMPLICITY Privilege Management Vulnerability Vulnerability(ICSA-16-194-02)	Vulnerability - level 3	Vuln
590150	GE Proficy GDS Blind XXE Vulnerability(ICSA-18-340-01)	Vulnerability - level 3	Vuln
590151	AVEVA Wonderware System Platform Vulnerability(ICSA-19-029-03)	Vulnerability - level 3	Vuln
590152	Schneider Electric ProClima Command Injection Multiple Vulnerabilities(ICSA-14-350-01)	Vulnerability - level 5	Vuln
590153	OSIsoft PI AF Server Input Validation Vulnerability Vulnerability(ICSA-16-166-02)	Vulnerability - level 3	Vuln
590154	Schneider Electric ProClima Multiple Vulnerabilities(ICSA-19-295-01)	Vulnerability - level 5	Vuln
590155	Schneider Electric Interactive Graphical SCADA System Software Vulnerability(ICSA-17-094-01)	Vulnerability - level 3	Vuln
590156	GE iFix Vulnerability(ICSA-18-282-01)	Vulnerability - level 3	Vuln
590158	OSIsoft Multiple Vulnerabilities(ICSA-13-225-02)	Vulnerability - level 3	Vuln
590159	OSIsoft PI Interface for DNP3 Improper Input Validation Multiple Vulnerabilities(ICSA-14-098-01)	Vulnerability - level 3	Vuln
590160	GE Proficy HMI/SCADA CIMPLICITY WebView Improper Input Validation Vulnerability(ICSA-13-170-01)	Vulnerability - level 5	Vuln
590161	GE Proficy Historian Web Administrator XSS Vulnerability(ICSA-11-243-02)	Potential Vulnerability - level 3	Practice
590162	HMS Industrial Networks eCatcher Vulnerability(ICSA-20-210-03)	Vulnerability - level 5	Vuln
590164	OSIsoft PI OPC DA Interface Buffer Overflow Vulnerability(ICSA-12-201-01)	Vulnerability - level 4	Vuln
590165	GE Proficy Historian ihDataArchiver Vulnerability(ICSA-12-032-01)	Vulnerability - level 5	Vuln
590166	GE Intelligent Platforms Proficy Cimplicity Multiple Vulnerabilities(ICSA-13-022-02)	Vulnerability - level 5	Vuln

590168	Delta Electronics Delta Industrial Automation PMSoft Vulnerability(ICS-18-270-04)	Vulnerability - level 3	Vuln
590169	Delta Industrial Automation TPEditor Multiple Vulnerabilities(ICS-18-284-03)	Vulnerability - level 3	Vuln
590170	Omron CX-One Multiple Vulnerabilities(ICS-18-100-02)	Vulnerability - level 3	Vuln
590171	OSIsoft PI Vision Vulnerability(ICS-19-043-01)	Vulnerability - level 3	Vuln
590172	GE Proficy HMI/SCADA Cimplicity Integer Overflow Vulnerability(ICS-12-341-01)	Potential Vulnerability - level 3	Practice
590173	Omron CX-One CX-Protocol Vulnerability(ICS-19-010-02)	Vulnerability - level 3	Vuln
590174	OSIsoft PI Web API Multiple Vulnerabilities(ICS-19-225-02)	Potential Vulnerability - level 3	Practice
590175	AVEVA InTouch Buffer Overflow Vulnerability(ICS-18-200-02)	Vulnerability - level 3	Vuln
590176	Omron Multiple Product Multiple Vulnerabilities(ICS-15-274-01)	Vulnerability - level 3	Vuln
590178	Pro-face GP-Pro EX HMI Multiple Vulnerabilities(ICS-16-096-01)	Potential Vulnerability - level 3	Practice
590179	GE Digital CIMPLICITY Vulnerability(ICS-20-098-02)	Vulnerability - level 3	Vuln
590180	GE Communicator Multiple Vulnerabilities(ICS-19-122-02)	Vulnerability - level 5	Vuln
590181	Rockwell Automation MicroLogix Controllers and RSLogix 500 Software Multiple Vulnerabilities(ICS-20-070-06)	Vulnerability - level 3	Vuln
590182	Rockwell Automation Allen-Bradley Stratix 5950 Vulnerability(ICS-20-072-03)	Potential Vulnerability - level 3	Practice
590183	Rockwell Automation Stratix 5400/5410/5700/8000/8300 and ArmorStratix 5700 Multiple Vulnerabilities(ICS-19-094-03)	Potential Vulnerability - level 3	Practice
590185	Rockwell Automation MicroLogix 1400 and CompactLogix 5370 Controllers Vulnerability(ICS-19-113-01)	Vulnerability - level 3	Vuln
590186	Rockwell Automation Stratix 5400/5410/5700 and ArmorStratix 5700 Vulnerability(ICS-19-094-02)	Potential Vulnerability - level 3	Practice
590187	Rockwell Automation Stratix 5950 Vulnerability(ICS-19-094-04)	Potential Vulnerability - level 3	Practice
590188	Rockwell Automation PanelView 5510 Vulnerability(ICS-19-190-02)	Vulnerability - level 3	Vuln
590189	Rockwell Automation CompactLogix 5370 Multiple Vulnerabilities(ICS-19-120-01)	Vulnerability - level 3	Vuln
590190	Siemens RUGGEDCOM, SCALANCE, SIMATIC, SINEMA (Update B) Multiple Vulnerabilities(ICS-20-105-05)	Vulnerability - level 3	Vuln
590191	Siemens SIMATIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update I) Vulnerability (ICS-19-099-06) (SSA-480230)	Vulnerability - level 4	Vuln
590193	Siemens Open Secure Sockets Layer (OpenSSL) (Update G) Multiple Vulnerabilities (ICS-14-198-03G)	Vulnerability - level 3	Vuln
590195	Siemens SIMATIC S7-300 CPUs and SINUMERIK Controller over Profinet (Update A) Vulnerability (ICS-20-070-02)	Vulnerability - level 4	Vuln
590196	Siemens SIMATIC S7 (Update B) Denial-of-Service Vulnerability(ICS-20-042-05)	Potential Vulnerability - level 4	Practice
590198	Siemens SIMATIC S7-200 SMART CPU Family Vulnerability(ICS-20-196-06)	Vulnerability - level 3	Vuln
590199	Siemens SCALANCE W700 and W1700 Vulnerability(ICS-19-344-01)	Vulnerability - level 3	Vuln
590200	Siemens SCALANCE X Switches Vulnerability (ICS-20-042-07, SSA-951513)	Vulnerability - level 3	Vuln
590202	Siemens Industrial Products (Update B) Vulnerability(ICS-20-252-07)	Potential Vulnerability - level 2	Practice
590203	Siemens SCALANCE X Switches (Update A) Vulnerability(ICS-19-225-03)	Potential Vulnerability - level 3	Practice
590204	Siemens SIMATIC S7-300 and S7-400 CPUs (Update C) Vulnerability(ICS-20-252-02)	Vulnerability - level 3	Vuln
590205	Siemens SICAM A8000 RTUs Vulnerability(ICS-20-224-08)	Vulnerability - level 3	Vuln
590209	Siemens LOGO! (Update A) Vulnerability(ICS-20-161-03)	Potential Vulnerability - level 3	Practice

590210	Siemens SIMATIC S7-1200 and S7-1500 CPU Families (Update A) Multiple Vulnerabilities(ICSA-19-344-06)	Vulnerability - level 3	Vuln
590212	Siemens ICS Device with OPC UA DoS Vulnerability(ICSA-19-099-03)	Vulnerability - level 3	Vuln
590213	Delta Electronics Delta Industrial Automation DOPSoft Vulnerability(ICSA-18-060-03)	Vulnerability - level 3	Vuln
590214	Delta Industrial Automation DOPSoft Multiple Vulnerabilities(ICSA-18-151-01)	Vulnerability - level 3	Vuln
590215	Delta Electronics Delta Industrial Automation TPEditor (Update A) Vulnerability(ICSA-18-137-04)	Vulnerability - level 3	Vuln
590216	Delta Electronics WPLSoft Multiple Vulnerabilities(ICSA-18-058-02)	Vulnerability - level 3	Vuln
590217	Delta Electronics ISPSOFT Vulnerability(ICSA-18-275-01)	Vulnerability - level 3	Vuln
590219	PTC Kepware KEPServerEX (Update A) Multiple Vulnerabilities(ICSA-20-352-02)	Vulnerability - level 3	Vuln
590220	Delta Electronics WPLSoft, ISPSOFT Multiple Vulnerabilities(ICSA-16-348-03)	Vulnerability - level 3	Vuln
590221	Ecava IntegraXor Multiple Vulnerabilities(ICSA-17-353-03)	Vulnerability - level 3	Vuln
590222	Ecava IntegraXor ActiveX Directory Traversal Vulnerability(ICSA-12-083-01)	Vulnerability - level 5	Vuln
590224	Siemens JT2Go (Update A) Multiple Vulnerabilities(ICSA-21-012-03)	Vulnerability - level 3	Vuln
590226	Softing Industrial Automation OPC Multiple Vulnerabilities(ICSA-20-210-02)	Vulnerability - level 3	Vuln
590227	Ecava Integraxor SCADA Server Multiple Vulnerabilities(ICSA-14-224-01)	Vulnerability - level 5	Vuln
590228	Ecava IntegraXor ActiveX Buffer Overflow Vulnerability(ICSA-13-036-02)	Vulnerability - level 5	Vuln
590229	Ecava IntegraXor DLL Vulnerability(ICSA-15-090-02)	Vulnerability - level 3	Vuln
590230	Ecava IntegraXor Multiple Vulnerabilities(ICSA-16-105-03)	Vulnerability - level 3	Vuln
590231	Ecava IntegraXor Vulnerability(ICSA-17-171-01)	Vulnerability - level 3	Vuln
590233	Rockwell Automation Logix5000 Programmable Automation Controller Buffer Overflow Vulnerability (Update B) Vulnerability(ICSA-16-343-05)	Potential Vulnerability - level 3	Practice
590234	Rockwell Automation ControlLogix 5580 and CompactLogix 5380 Vulnerability(ICSA-17-094-05)	Vulnerability - level 3	Vuln
590235	Rockwell Automation Allen-Bradley CompactLogix and Compact GuardLogix (Update A) Vulnerability(ICSA-18-172-02)	Vulnerability - level 3	Vuln
590236	Rockwell Automation MicroLogix 1400 Controllers and 1756 ControlLogix Communications Modules Vulnerability (ICSA-18-310-02)	Vulnerability - level 3	Vuln
590237	Rockwell Automation EtherNet/IP Web Server Modules Vulnerability(ICSA-19-036-02)	Potential Vulnerability - level 3	Practice
590238	Rockwell Automation ControlLogix PLC Multiple Vulnerabilities(ICSA-13-011-03)	Vulnerability - level 3	Vuln
590239	Rockwell Automation Micrologix 1100 and 1400 PLC Systems (Update A) Multiple Vulnerabilities(ICSA-15-300-03A)	Vulnerability - level 3	Vuln
590240	Rockwell Automation MicroLogix 1100 PLC Overflow Vulnerability Vulnerability(ICSA-16-026-02)	Vulnerability - level 3	Vuln
590241	Siemens SIMATIC S7-1500 (Update A) Vulnerability(ICSA-20-042-11)	Vulnerability - level 3	Vuln
590243	Siemens SIMATIC S7-400 CPU (Update A) Vulnerability(ICSA-18-137-03)	Vulnerability - level 3	Vuln
590244	Siemens SIMATIC Communication Processor Vulnerability (Update B) Vulnerability(ICSA-15-335-03A)	Vulnerability - level 5	Vuln
590245	Siemens S7-300/400 PLC (Update E) Multiple Vulnerabilities(ICSA-16-348-05)	Vulnerability - level 4	Vuln

590246	Siemens SIMATIC CP 343-1/CP 443-1 Modules and SIMATIC S7-300/S7-400 CPUs (Update B) Multiple Vulnerabilities(ICSA-16-327-02)	Vulnerability - level 4	Vuln
590247	Siemens SIMATIC, SINUMERIK, and PROFINET IO (Update D) Vulnerability(ICSA-18-079-02)	Vulnerability - level 3	Vuln
590248	Siemens SCALANCE And SIMATIC (Update D) Vulnerability(ICSA-20-105-07)	Vulnerability - level 3	Vuln
590249	Siemens Industrial Products (Update A) Vulnerability(ICSA-18-023-02)	Vulnerability - level 3	Vuln
590250	Siemens S7-400 CPUs (Update B) Multiple Vulnerabilities (SSA-113131, ICSA-18-317-02)	Potential Vulnerability - level 4	Practice
590252	Rockwell Automation Logix Controllers Vulnerability(ICSA-21-056-03)	Vulnerability - level 3	Vuln
590253	ABB PCM600 Multiple Vulnerabilities(ICSA-16-152-02)	Vulnerability - level 3	Vuln
590254	ABB Panel Builder 800 DLL Hijacking Vulnerability (Update A) Vulnerability(ICSA-16-077-01)	Vulnerability - level 3	Vuln
590255	Red Lion Crimson 3.1 Multiple Vulnerabilities(ICSA-21-005-04)	Vulnerability - level 3	Vuln
590256	Ecava IntegraXor SQL injection Vulnerability(ICSA-17-031-02)	Vulnerability - level 3	Vuln
590257	Siemens JT2Go Multiple Vulnerabilities(ICSA-21-040-06)	Vulnerability - level 3	Vuln
590258	Progea Movicon SCADA Information Disclosure Vulnerability (ICSA-14-105-01)	Vulnerability - level 3	Vuln
590260	Ecava Sdn Bhd IntegraXor Project Directory Information Disclosure Vulnerability(ICSA-14-008-01)	Vulnerability - level 3	Vuln
590261	Progea Movicon Memory Corruption Vulnerability (ICSA-12-131-01)	Vulnerability - level 3	Vuln
590263	Ecava IntegraXor Guest Account Information Disclosure Vulnerability(ICSA-14-091-01)	Vulnerability - level 3	Vuln
590265	Omron CX-One Multiple Vulnerabilities(ICSA-18-338-01)	Vulnerability - level 3	Vuln
590266	3S-Smart CODESYS GmbH V3 Multiple Vulnerabilities (ICSA-18-352-04)	Vulnerability - level 3	Vuln
590267	AzeoTech DAQFactory Multiple Vulnerabilities(ICSA-17-241-01)	Vulnerability - level 3	Vuln
590271	Fuji Electric Alpha5 Smart Loader (Update A) Multiple Vulnerabilities(ICSA-18-270-02)	Vulnerability - level 3	Vuln
590272	Unitronics VisiLogic OPLC IDE vlp File Parsing Stack Buffer Overflow Vulnerability Multiple Vulnerabilities(ICSA-16-175-02)	Vulnerability - level 3	Vuln
590273	Eaton ELCSOft buffer overflow Vulnerability(ICSA-18-065-03)	Vulnerability - level 3	Vuln
590278	7-Technologies IGSS Buffer Overflow Vulnerability(ICSA-11-355-01)	Vulnerability - level 3	Vuln
590279	7-Technologies Interactive Graphical SCADA Vulnerability(ICSA-11-353-01)	Vulnerability - level 5	Vuln
590282	MatrikonOPC Explorer Improper Authorization Vulnerability(ICSA-18-130-01)	Vulnerability - level 3	Vuln
590283	MatrikonOPC for DNP Unhandled C++ Exception Vulnerability(ICSA-14-329-01)	Vulnerability - level 3	Vuln
590284	Inductive Automation Ignition Multiple Vulnerabilities(ICSA-15-090-01)	Vulnerability - level 3	Vuln
590287	Advantech WebAccess/SCADA WADashboard component Vulnerability(ICSA-20-289-01)	Vulnerability - level 3	Vuln
590288	Inductive Automation Ignition (Update B) Multiple Vulnerabilities(ICSA-20-147-01)	Vulnerability - level 3	Vuln
590289	3S-Smart CODESYS GmbH Gateway Server Buffer Overflow Vulnerability(ICSA-15-258-02)	Vulnerability - level 4	Vuln
590290	3S-Smart CODESYS Runtime Toolkit NULL Pointer Dereference Vulnerability (ICSA-14-030-01)	Vulnerability - level 3	Vuln
590291	3S-Smart CODESYS GmbH Gateway Use After Free Vulnerability (ICSA-13-142-01)	Vulnerability - level 5	Vuln
590292	MICROSYS PROMOTIC Memory Corruption Vulnerability (ICSA-16-026-01)	Vulnerability - level 3	Vuln

590294	MICROSYS PROMOTIC Stack Buffer Overflow Vulnerability(ICS-15-062-01)	Vulnerability - level 3	Vuln
590295	MICROSYS PROMOTIC Use After Free Vulnerability (ICS-12-102-03)	Vulnerability - level 3	Vuln
590296	Delta Electronics ISPSOft Arbitrary Code Execution Vulnerability(ICS-21-021-01)	Vulnerability - level 3	Vuln
590298	Software Toolbox Top Server Resource Exhaustion Vulnerability(ICS-15-055-01)	Vulnerability - level 3	Vuln
590299	Top Server OPC Improper Input Validation Vulnerability (ICS-13-234-02)	Vulnerability - level 3	Vuln
590300	SearchBlox File Exfiltration Vulnerability(ICS-15-337-01)	Vulnerability - level 3	Vuln
590301	Pilz PNOZmulti Configurator Vulnerability(ICS-19-010-03)	Vulnerability - level 1	Vuln
590302	Inductive Automation Ignition DoS Vulnerability(ICS-20-112-01)	Vulnerability - level 3	Vuln
590303	3S-Smart CODESYS GmbH Runtime Toolkit Null Pointer Dereference Vulnerability(ICS-15-288-01)	Vulnerability - level 3	Vuln
590304	3S-Smart CODESYS GmbH Gateway-Server (Update A) Multiple Vulnerabilities (ICS-13-050-01A)	Vulnerability - level 5	Vuln
590305	3S-Smart CODESYS GmbH Gateway Null Pointer Exception Vulnerability(ICS-15-293-03)	Vulnerability - level 3	Vuln
590307	3S-Smart CODESYS GmbH Web Server Multiple Vulnerabilities (ICS-17-087-02)	Vulnerability - level 3	Vuln
590308	Eaton ELCSOft Programming Software Memory Multiple Vulnerabilities(ICS-16-182-01)	Vulnerability - level 3	Vuln
590309	xArrow Multiple Vulnerabilities(ICS-12-145-02)	Vulnerability - level 3	Vuln
590310	Unitronics VisiLogic OPLC IDE (Update A) Multiple Vulnerabilities(ICS-15-274-02A)	Vulnerability - level 5	Vuln
590311	Advantech WebAccess Node privilege escalation Vulnerability(ICS-20-261-01)	Vulnerability - level 3	Vuln
590312	Inductive Automation Ignition 8 sensitive Information Disclosure Vulnerability(ICS-20-212-01)	Vulnerability - level 3	Vuln
590313	Rockwell Automation FactoryTalk Services Platform Use of Password Hash with Insufficient Computational Effort Vulnerability(ICS-21-054-01)	Vulnerability - level 3	Vuln
590314	Wonderware Information Server Multiple Vulnerabilities(ICS-12-062-01)	Vulnerability - level 3	Vuln
590315	Wonderware Information Server Multiple Vulnerabilities(ICS-13-113-01)	Vulnerability - level 5	Vuln
590316	Fuji Electric FRENIC Devices (Update A) Multiple Vulnerabilities (ICS-18-270-03)	Potential Vulnerability - level 5	Practice
590320	InduSOft ISSymbol ActiveX Control Buffer Overflow Vulnerability(ICS-11-273-02)	Vulnerability - level 5	Vuln
590323	Rockwell Automation 1734-AENTR Series B and Series C Multiple Vulnerabilities(ICS-21-063-01)	Vulnerability - level 3	Vuln
590324	Rockwell Automation CompactLogix 5370 and ControlLogix 5570 Controllers (Update A) Vulnerability(ICS-21-061-02)	Vulnerability - level 3	Vuln
590325	Rockwell Automation Hardware Logix Controllers (Update A) Vulnerability(ICS-21-056-03)	Potential Vulnerability - level 3	Practice
590326	Rockwell Automation Allen-Bradley Micrologix 1100 Vulnerability(ICS-21-047-02)	Vulnerability - level 3	Vuln
590327	Rockwell Automation MicroLogix 1400 (Update A) Vulnerability(ICS-21-033-01)	Potential Vulnerability - level 3	Practice
590329	National Instruments CompactRIO Vulnerability(ICS-20-338-01)	Vulnerability - level 3	Vuln
590330	Schneider Electric EcoStruxure Building Operation (EBO) Multiple Vulnerabilities(ICS-21-063-02)	Vulnerability - level 3	Vuln
590331	AutomationDirect C-More, C-More Micro, Do-more Designer, DirectSOFT (Update B) DLL Hijacking Vulnerability(ICS-17-313-01)	Vulnerability - level 5	Vuln
590333	Rockwell Automation PowerFlex 525 AC Drives Vulnerability(ICS-19-087-01)	Vulnerability - level 3	Vuln

590335	Rockwell Automation Allen-Bradley Stratix 5400 and 5410 Packet Corruption Vulnerability Vulnerability (ICSA-16-175-01)	Potential Vulnerability - level 4	Practice
590336	Rockwell Micrologix 1400 DNP3 DOS Vulnerability Vulnerability(ICSA-14-254-02)	Potential Vulnerability - level 3	Practice
590337	Rockwell Allen-Bradley MicroLogix, SLC 500, and PLC-5 Fault Generation Vulnerability (Update B) Vulnerability(ICSA-12-342-01B)	Potential Vulnerability - level 3	Practice
590340	Rockwell Automation MicroLogix 1400 SNMP Credentials Vulnerability Vulnerability(ICSA-16-224-01)	Vulnerability - level 3	Vuln
590341	Rockwell Automation Allen-Bradley Stratix 5950 Multiple Vulnerabilities (ICSA-18-184-01)	Potential Vulnerability - level 4	Practice
590342	Rockwell Automation Allen-Bradley Stratix and ArmorStratix Multiple Vulnerabilities (ICSA-17-208-04)	Potential Vulnerability - level 4	Practice
590344	Rockwell Automation Allen-Bradley MicroLogix 1400 Controllers Vulnerability(ICSA-18-009-01)	Potential Vulnerability - level 3	Practice
590345	Rockwell Automation Allen-Bradley MicroLogix 1100 and 1400 Multiple Vulnerabilities(ICSA-17-115-04)	Potential Vulnerability - level 3	Practice
590346	Rockwell Automation PanelView Plus 6 700-1500 Vulnerability (ICSA-17-157-01)	Potential Vulnerability - level 4	Practice
590347	Rockwell Automation MicroLogix 1100 and 1400 Multiple Vulnerabilities(ICSA-16-336-06)	Vulnerability - level 3	Vuln
590348	Rockwell Automation Stratix Denial-of-Service and Memory Leak Multiple Vulnerabilities (ICSA-16-287-04)	Potential Vulnerability - level 4	Practice
590349	Rockwell Automation Stratix 5900 Multiple Vulnerabilities (ICSA-17-094-04)	Vulnerability - level 5	Vuln
590351	Rockwell Automation MicroLogix 1100 Controllers Vulnerability(ICSA-17-138-03)	Vulnerability - level 3	Vuln
590352	"B and R" Automation Studio Multiple Vulnerabilities(ICSA-20-093-01)	Vulnerability - level 3	Vuln
590354	Johnson Controls exacqVision (Update A) Vulnerability(ICSA-20-170-01)	Vulnerability - level 5	Vuln
590356	Eaton Intelligent Power Manager Multiple Vulnerabilities(ICSA-21-110-06)	Vulnerability - level 5	Vuln
590357	Siemens RUGGEDCOM ROX II Multiple Vulnerabilities(ICSA-21-040-04)	Vulnerability - level 3	Vuln
590358	Siemens SCALANCE W780 and W740 Vulnerability(ICSA-21-040-07)	Vulnerability - level 3	Vuln
590359	Siemens SCALANCE X Switches (Update A) Multiple Vulnerabilities(ICSA-21-012-02,ICSA-21-012-05)	Vulnerability - level 3	Vuln
590360	Siemens Embedded TCP/IP Stack AMNESIA:33 (Update C) Vulnerability (ICSA-20-343-05)	Vulnerability - level 3	Vuln
590361	Siemens Climatix (Update A) Multiple Vulnerabilities(ICSA-20-105-04)	Potential Vulnerability - level 3	Practice
590362	Siemens Industrial Real-Time (IRT) Devices (Update E) Vulnerability(ICSA-19-283-01)	Vulnerability - level 3	Vuln
590363	Siemens SCALANCE X Switches, RUGGEDCOM WiMAX, RFID 181-EIP, and SIMATIC RF182C (Update D) Heap Overflow Vulnerability(ICSA-18-165-01)	Vulnerability - level 3	Vuln
590364	Siemens SICAM A8000 Remote Terminal Unit (RTU) Insecure Secure Sockets Layer (SSL) Configuration Vulnerability (ICSA-20-343-07)	Vulnerability - level 3	Vuln
590366	Siemens SIPROTEC 5 (Update C) Multiple Vulnerabilities(ICSA-19-190-05)	Potential Vulnerability - level 3	Practice
590367	Siemens SCALANCE Privilege Escalation (Update A) Multiple Vulnerabilities(ICSA-13-149-01)	Vulnerability - level 3	Vuln
590368	Siemens SCALANCE X Switches Authentication Bypass Vulnerability(ICSA-20-014-03)	Potential Vulnerability - level 3	Practice
590369	Siemens SIMATIC Ident MV440 Family (Update A) Multiple Vulnerabilities(ICSA-19-162-02)	Vulnerability - level 3	Vuln

590370	Siemens TIM 3V-IE and 4R-IE Family Devices Vulnerability(ICSA-20-105-09)	Potential Vulnerability - level 3	Practice
590371	Siemens SCALANCE Products (Update A) Multiple Vulnerabilities(ICSA-19-227-03)	Vulnerability - level 3	Vuln
590372	Siemens S7-1200 and S7-200 SMART CPUs (Update B) Vulnerability(ICSA-19-318-02)	Vulnerability - level 3	Vuln
590373	Siemens SIMOCODE pro V EIP Denial-of-Service Vulnerability(ICSA-19-099-01)	Potential Vulnerability - level 3	Practice
590374	Siemens LOGO! 8 BM Multiple Vulnerabilities(ICSA-20-343-10)	Vulnerability - level 3	Vuln
590376	Siemens CP1604 and CP1616 (Update A) Multiple Vulnerabilities(ICSA-19-043-06)	Potential Vulnerability - level 3	Practice
590377	Siemens SIMATIC Controller Web Servers Vulnerability(ICSA-20-343-09)	Vulnerability - level 3	Vuln
590378	Siemens LOGO! (Update A) Multiple Vulnerabilities(ICSA-17-243-02)	Vulnerability - level 3	Vuln
590379	Siemens SCALANCE X (Update B) Mirror Port Isolation Vulnerability (ICSA-19-085-01)	Vulnerability - level 3	Vuln
590381	Siemens SCALANCE X (Update B) Vulnerability(ICSA-19-162-04)	Vulnerability - level 3	Vuln
590382	Siemens RUGGEDCOM ROX II Multiple Vulnerabilities(ICSA-19-099-05)	Potential Vulnerability - level 3	Practice
590383	Siemens TIM 1531 IRC Modules Missing Authentication Vulnerability(ICSA-18-352-05)	Vulnerability - level 3	Vuln
590385	Siemens SCALANCE X Switches (Update A) Multiple Vulnerabilities(ICSA-18-163-02)	Vulnerability - level 3	Vuln
590386	Siemens SIMATIC S7-300 CPUs and SINUMERIK Controller: Denial-of-Service Vulnerability(ICSA-20-315-04)	Vulnerability - level 4	Vuln
590387	Siemens SCALANCE W1750D Multiple Vulnerabilities(ICSA-19-134-07)	Vulnerability - level 5	Vuln
590389	Siemens SCALANCE S-600 (Update B) Multiple Vulnerabilities (ICSA-20-042-10)	Vulnerability - level 3	Vuln
590390	Siemens SIPROTEC 4 and SIPROTEC Compact Vulnerability(ICSA-20-042-12)	Potential Vulnerability - level 3	Practice
590391	Siemens RUGGEDCOM ROS Multiple Vulnerabilities(ICSA-19-344-03)	Potential Vulnerability - level 3	Practice
590392	Siemens SIMATIC RF6XXR Multiple Vulnerabilities(ICSA-19-192-04)	Vulnerability - level 3	Vuln
590393	Siemens SIMATIC TDC CP51M1 Denial-of-Service Vulnerability(ICSA-19-253-05)	Vulnerability - level 3	Vuln
590395	Siemens SIMATIC HMI Panels Clear Text Transmission Vulnerability(ICSA-20-196-04)	Vulnerability - level 3	Vuln
590396	Siemens SIMATIC Products (Update B) MITM Vulnerability(ICSA-19-344-04)	Vulnerability - level 3	Vuln
590397	Siemens SINEMA Server Incorrect Session Validation Vulnerability(ICSA-20-014-02)	Vulnerability - level 5	Vuln
590398	Siemens KTK, SIDOOR, SIMATIC, and SINAMICS (Update B) DoS Vulnerability(ICSA-20-105-08)	Vulnerability - level 4	Vuln
590399	Siemens PROFINET-IO Stack (Update D) DoS Vulnerability(ICSA-20-042-04)	Vulnerability - level 4	Vuln
590400	Siemens PROFINET Devices (Update I) DoS Vulnerability(ICSA-19-283-02)	Vulnerability - level 4	Vuln
590401	Siemens Industrial Products (Update Q) DoS Vulnerability(ICSA-17-339-01)	Vulnerability - level 4	Vuln
590403	Siemens PROFINET DCP (Update S) Multiple Vulnerabilities(ICSA-17-129-02)	Vulnerability - level 3	Vuln
590404	OSIsoft PI System (Update A) Multiple Vulnerabilities(ICSA-20-133-02)	Vulnerability - level 3	Vuln
590405	WECON PLC Editor Multiple Vulnerabilities(ICSA-20-310-01)	Vulnerability - level 3	Vuln
590406	LCDS LAquis SCADA Multiple Vulnerabilities(ICSA-20-119-01)	Vulnerability - level 3	Vuln

590407	LAquis SCADA LQS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability(ICS-20-287-02)	Vulnerability - level 3	Vuln
590408	Schneider Electric ProClima ActiveX Control Vulnerability(ICS-15-335-02)	Vulnerability - level 3	Vuln
590409	Schneider Electric C-Bus Toolkit Multiple Vulnerabilities(ICS-21-105-01)	Vulnerability - level 3	Vuln
590410	Schneider Electric IGSS SCADA Software Multiple Vulnerabilities(ICS-21-070-01)	Vulnerability - level 5	Vuln
590411	Rockwell Automation FactoryTalk AssetCentre Multiple Vulnerabilities(ICS-21-091-01)	Vulnerability - level 3	Vuln
590412	Siemens TIA Administrator improper access controls Vulnerability(ICS-21-040-05)	Vulnerability - level 3	Vuln
590413	Delta Industrial Automation TPEditor Multiple Vulnerabilities(ICS-20-219-04)	Vulnerability - level 3	Vuln
590414	Rockwell Automation DriveTools SP and Drives AOP privilege escalation Vulnerability(ICS-21-042-02)	Vulnerability - level 3	Vuln
590415	Siemens LOGO! Soft Comfort Multiple Vulnerabilities(ICS-21-103-09)	Vulnerability - level 3	Vuln
590416	Siemens LOGO! Soft Comfort Multiple Vulnerabilities(ICS-20-343-10)	Vulnerability - level 3	Vuln
590418	KUKA Sim Pro Improper Enforcement of Message Integrity During Transmission in a Communication Channel Vulnerability(ICS-20-098-05)	Vulnerability - level 3	Vuln
590419	Johnson Controls Sensormatic Electronics American Dynamics victor Web Client Vulnerability(ICS-20-324-01)	Vulnerability - level 3	Vuln
590421	Johnson Controls Software House C-CURE 9000 and American Dynamics victor VMS Vulnerability(ICS-20-142-01)	Vulnerability - level 3	Vuln
590422	Delta Industrial Automation DOPSoft (Update A) Multiple Vulnerabilities(ICS-20-182-01)	Vulnerability - level 3	Vuln
590423	Delta Industrial Automation COMMGR Buffer Overflow Vulnerability(ICS-21-110-03)	Vulnerability - level 3	Vuln
590424	Delta Electronics CNCSoft ScreenEditor arbitrary code execution Vulnerability(ICS-21-110-04)	Vulnerability - level 3	Vuln
590425	Rockwell Automation Connected Components Workbench Multiple Vulnerabilities(ICS-21-133-01)	Vulnerability - level 3	Vuln
590426	Schneider Electric PLC Simulator for EcoStruxure Control Expert DoS Vulnerability(ICS-20-315-03)	Potential Vulnerability - level 3	Practice
590429	Opto 22 SoftPAC Project Multiple Vulnerabilities(ICS-20-135-01)	Vulnerability - level 3	Vuln
590430	WECON LeviStudio Buffer Overflow Multiple Vulnerabilities(ICS-16-189-01)	Vulnerability - level 3	Vuln
590431	Siemens SIMATIC Panels Multiple Vulnerabilities(ICS-18-317-08)	Vulnerability - level 3	Vuln
590432	OSIsoft PI Web API 2019 cross-site scripting Vulnerability(ICS-20-163-01)	Vulnerability - level 3	Vuln
590433	OSIsoft PI Vision Multiple Vulnerabilities(ICS-20-315-02)	Vulnerability - level 3	Vuln
590434	Advantech WebAccess/SCADA cross-site scripting Vulnerability(ICS-21-075-01)	Vulnerability - level 3	Vuln
590436	Luxion KeyShot (Update A) Multiple Vulnerabilities(ICS-21-035-01)	Vulnerability - level 3	Vuln
590437	FATEK Automation FvDesigner Multiple Vulnerabilities(ICS-21-056-02)	Vulnerability - level 3	Vuln
590438	Advantech WebAccess SCADA privilege escalation Vulnerability(ICS-21-103-02)	Vulnerability - level 5	Vuln
590439	Schneider Electric IGSS SCADA Software Multiple Vulnerabilities(ICS-20-084-02)	Vulnerability - level 3	Vuln
590440	Siemens SIMATIC HMI Comfort Panels and SIMATIC HMI KTP Mobile Panels Vulnerability (ICS-21-033-02)	Potential Vulnerability - level 5	Practice
590441	Schneider Electric SoMachine Basic XML External Entity (XXE) Vulnerability(ICS-21-103-01)	Vulnerability - level 3	Vuln

590442	Siemens SIMATIC HMI Products (Update A) Multiple Vulnerabilities (ICSA-20-252-06)	Vulnerability - level 5	Vuln
590444	Siemens LOGO!8 Devices Multiple Vulnerabilities (ICSA-19-162-03)	Vulnerability - level 3	Vuln
590445	Siemens EN100 Ethernet Module (Update A) Multiple Vulnerabilities (ICSA-19-344-07)	Potential Vulnerability - level 3	Practice
590446	FATEK Automation WinProLadder integer underflow Vulnerability(ICSA-21-098-01)	Vulnerability - level 3	Vuln
590449	Advantech WebAccess Node Multiple Vulnerabilities(ICSA-20-128-01)	Vulnerability - level 3	Vuln
590450	Schneider Electric IGSS Multiple Vulnerabilities(ICSA-21-159-04)	Vulnerability - level 3	Vuln
590451	AVEVA InTouch Cleartext Password in WindowViewer Diagnostic Memory Dumps Vulnerability(ICSA-21-159-03)	Vulnerability - level 3	Vuln
590452	Rockwell Automation FactoryTalk Services Platform Authentication Bypass Vulnerability(ICSA-21-161-01)	Vulnerability - level 3	Vuln
590454	WAGO Series 750-88x and 750-352 (Update A) Denial of Service (DoS) Vulnerability (ICSA-20-308-01)	Vulnerability - level 3	Vuln
590455	WAGO I/O-CHECK Multiple Vulnerabilities (ICSA-20-065-01)	Potential Vulnerability - level 5	Practice
590456	WAGO Industrial Managed Switches 852-303, 852-1305, and 852-1505 Multiple Vulnerabilities (ICSA-19-164-02)	Vulnerability - level 5	Vuln
590457	WAGO Series 750-88x and 750-87x Use of Hard-coded Credentials Vulnerability (ICSA-19-106-02)	Vulnerability - level 3	Vuln
590459	WAGO 750 Series Denial of Service (DoS) Vulnerability (ICSA-18-088-01)	Potential Vulnerability - level 3	Practice
590460	WAGO Ethernet Web-based Management Authentication Bypass Vulnerability Vulnerability (ICSA-16-357-02)	Vulnerability - level 3	Vuln
590461	WAGO IO 758 Default Linux Credentials Vulnerability (ICSA-12-249-02)	Potential Vulnerability - level 5	Practice
590462	Omron PLC CJ Series DoS Vulnerability (ICSA-20-063-03)	Vulnerability - level 3	Vuln
590463	Omron PLC CJ and CS Series Multiple Vulnerabilities (ICSA-19-346-02)	Vulnerability - level 3	Vuln
590464	Omron PLC CJ, CS and NJ Series Vulnerability (ICSA-19-346-03)	Vulnerability - level 3	Vuln
590465	Advantech WebAccess/SCADA Multiple Vulnerabilities(ICSA-21-168-03)	Vulnerability - level 3	Vuln
590466	Omron NS Series HMI Multiple Vulnerabilities (ICSA-14-203-01)	Vulnerability - level 3	Vuln
590467	Omron CJ2M,CJ2H Series PLC Multiple Vulnerabilities (ICSA-15-274-01)	Vulnerability - level 3	Vuln
590468	Schneider Electric EcoStruxure Control Expert Software Multiple Vulnerabilities(ICSA-21-194-02)	Vulnerability - level 3	Vuln
590469	Schneider Electric Web Server on Modicon M340 Multiple Vulnerabilities (ICSA-21-005-01)	Potential Vulnerability - level 3	Practice
590470	Schneider Electric Easergy T300 Multiple Vulnerabilities(ICSA-20-343-03)	Potential Vulnerability - level 3	Practice
590471	Schneider Electric Modicon M221 Programmable Logic Controller Multiple Vulnerabilities (ICSA-20-343-04)	Potential Vulnerability - level 3	Practice
590472	Schneider Electric Modicon Controllers (Update A) DoS Vulnerability(ICSA-20-016-01)	Vulnerability - level 3	Vuln
590473	Schneider Electric Modicon Controllers (Update A) Multiple Vulnerabilities(ICSA-20-016-01)	Vulnerability - level 3	Vuln
590474	Schneider Electric Modicon Ethernet Serial RTU Multiple Vulnerabilities (ICSA-20-044-01)	Potential Vulnerability - level 3	Practice
590475	Schneider Electric Magelis HMI Panels DoS Vulnerability (ICSA-20-044-02)	Potential Vulnerability - level 3	Practice
590476	Schneider Electric Modicon Controllers Multiple Vulnerabilities(ICSA-21-194-02)	Vulnerability - level 3	Vuln
590477	Schneider Electric Modicon Controllers DoS Vulnerability(ICSA-19-183-01)	Vulnerability - level 3	Vuln

590478	Schneider Electric EVLink Parking Multiple Vulnerabilities (ICSA-19-031-01)	Vulnerability - level 5	Vuln
590480	Schneider Electric Modicon M221 Insufficient Verification of Data Authenticity Vulnerability(ICSA-18-324-02)	Vulnerability - level 3	Vuln
590481	Schneider Electric Modicon M340 PLC (Update A) buffer overflow Vulnerability(ICSA-17-054-03)	Vulnerability - level 3	Vuln
590482	Schneider Electric PowerLogic PM5560 Cross Protocol Injection Vulnerability(ICSA-18-240-03)	Potential Vulnerability - level 3	Practice
590483	Schneider Electric Modicon M221 Multiple Vulnerabilities (ICSA-18-240-02,ICSA-18-240-01)	Vulnerability - level 3	Vuln
590484	Schneider Electric Modicon Premium, Modicon Quantum, Modicon M340, and Modicon BMXNOR0200 Multiple Vulnerabilities (ICSA-18-086-01)	Vulnerability - level 5	Vuln
590485	Schneider Electric PLCs (Update B) Multiple Vulnerabilities (ICSA-13-077-01B)	Vulnerability - level 3	Practice
590486	Schneider Electric Modicon M221 PLCs Multiple Vulnerabilities(ICSA-17-103-02A)	Vulnerability - level 3	Vuln
590487	Schneider Electric Modicon PLCs Multiple Vulnerabilities (ICSA-17-089-02)	Vulnerability - level 3	Vuln
590488	Schneider Electric Modicon PLCs Insufficiently Protected Credentials Vulnerability (ICSA-17-089-02)	Vulnerability - level 3	Vuln
590490	Schneider Electric PowerLogic PM8ECC Cross-Site Scripting (XSS) Vulnerability Vulnerability (ICSA-16-173-02)	Vulnerability - level 3	Vuln
590491	Schneider Electric ETG3000 FactoryCast HMI Gateway Multiple Vulnerabilities (ICSA-15-020-02)	Potential Vulnerability - level 5	Practice
590492	Schneider Electric Modicon M340 Buffer Overflow Vulnerability Vulnerability (ICSA-15-351-01)	Vulnerability - level 5	Vuln
590493	Schneider Electric Modicon PLC Multiple Vulnerabilities (ICSA-15-246-02)	Potential Vulnerability - level 3	Practice
590494	Panasonic FPWIN Pro XML external entity (XXE) injection Vulnerability(ICSA-21-180-03)	Vulnerability - level 3	Vuln
590495	AVEVA System Platform (Update A) Multiple Vulnerabilities(ICSA-21-180-05)	Vulnerability - level 3	Vuln
590496	Siemens UMC Stack (Update H) Multiple Vulnerabilities(ICSA-20-196-05)	Vulnerability - level 3	Vuln
590498	Sensormatic Electronics C-CURE 9000 Improper Input Validation Vulnerability(ICSA-21-182-02)	Vulnerability - level 3	Vuln
590499	Swisslog Healthcare Translogic Pneumatic Tube Systems Multiple Vulnerabilities (ICSMA-21-215-01)	Vulnerability - level 4	Vuln
590501	Siemens JT2Go Multiple Vulnerabilities(ICSA-21-194-15)	Vulnerability - level 3	Vuln
590502	Beckhoff Embedded PC Images and TwinCAT Components Multiple Vulnerabilities (ICSA-16-278-02)	Potential Vulnerability - level 5	Practice
590503	ABB Relion 650 and 670 Series Denial of Service (DoS) Vulnerability (ICSA-19-330-02)	Vulnerability - level 3	Vuln
590504	ABB Relion 670 Series Path Traversal Vulnerability (ICSA-19-330-01)	Potential Vulnerability - level 3	Practice
590505	ABB GATE-E2 Multiple Vulnerabilities (ICSA-18-352-01)	Vulnerability - level 3	Vuln
590506	ABB FOX515T Local File Inclusion Vulnerability (ICSA-17-304-01)	Vulnerability - level 3	Vuln
590507	Advantech R-SeeNet SQL Injection Vulnerability(ICSA-20-289-02)	Vulnerability - level 3	Vuln
590508	Siemens Interniche IP-Stack Multiple Vulnerabilities (SSA-789208)	Vulnerability - level 3	Vuln
590509	Schneider Electric Modicon Controllers Use of Insufficiently Random Values Vulnerability (ICSA-19-136-01)	Vulnerability - level 3	Vuln
590510	Siemens Automation License Manager DoS Vulnerability(ICSA-21-222-02)	Potential Vulnerability - level 3	Practice
590513	Cognex In-Sight OPC Server Local Privilege Escalation Vulnerability (ICSA-21-224-01)	Vulnerability - level 3	Vuln
590514	Siemens JT2Go Multiple Vulnerabilities (ICSA-21-222-03)	Vulnerability - level 3	Vuln

590515	LCDS LAquis SCADA Cross-site Scripting Vulnerability (ICSA-21-208-04)	Vulnerability - level 3	Vuln
590516	Schneider Electric Modicon X80 information disclosure Vulnerability (ICSA-21-159-05)	Vulnerability - level 3	Vuln
590518	Schneider Electric homeLynk Controller (Update A) Multiple Vulnerabilities (ICSA-17-019-01A)	Vulnerability - level 5	Vuln
590520	ABB CP651 HMI Use of Hard-coded Credentials Vulnerability (ICSA-19-178-02)	Vulnerability - level 3	Vuln
590521	ABB M2M ETHERNET Improper Authentication Vulnerability (ICSA-18-352-07)	Vulnerability - level 3	Vuln
590522	ABB VSN300 WiFi Logger Card Multiple Vulnerabilities (ICSA-17-192-03)	Vulnerability - level 3	Vuln
590523	Advantech WebAccess Supervisory control and data acquisition (SCADA) Multiple Vulnerabilities (ICSA-21-217-04)	Vulnerability - level 3	Vuln
590525	xArrow SCADA Multiple Vulnerabilities (ICSA-21-229-03)	Vulnerability - level 3	Vuln
590526	Horner Automation Cscape Multiple Vulnerabilities (ICSA-21-224-02)	Vulnerability - level 3	Vuln
590527	Delta Electronics DIAScreen Multiple Vulnerabilities (ICSA-21-208-05)	Vulnerability - level 3	Vuln
590528	Siemens JT Utilities Multiple Vulnerabilities (ICSA-21-194-09)	Vulnerability - level 1	Vuln
590529	Horner Automation Cscape Multiple Vulnerabilities (ICSA-21-112-01)	Vulnerability - level 3	Vuln
590531	Texas Instruments SimpleLink Multiple Vulnerabilities (ICSA-21-119-01)	Vulnerability - level 3	Vuln
590532	Exacq Technologies exacqVision Web Service Insufficient validation Vulnerability (ICSA-21-180-01)	Vulnerability - level 3	Vuln
590533	Siemens SIMATIC S7-PLCSIM Multiple Vulnerabilities (ICSA-21-068-01)	Vulnerability - level 3	Vuln
590534	Delta Electronics TPEditor Buffer Overflow Vulnerability (ICSA-21-236-03)	Vulnerability - level 3	Vuln
590535	Mitsubishi Electric GT SoftGOT2000 Denial of Service (DoS) Vulnerability (ICSA-21-208-02)	Vulnerability - level 3	Vuln
590536	Advantech WebAccess Buffer Overflow Vulnerability (ICSA-20-086-01)	Vulnerability - level 3	Vuln
590537	Exacq Technologies exacqVision Enterprise Manager Cross-site Scripting Vulnerability (ICSA-21-180-02)	Vulnerability - level 3	Vuln
590538	Mitsubishi Electric FA engineering software products Multiple Vulnerabilities (ICSA-21-049-02)	Vulnerability - level 3	Vuln
590540	Advantech WebAccess/NMS Multiple Vulnerabilities (ICSA-20-098-01)	Vulnerability - level 5	Vuln
590541	Schneider Electric EcoStruxure IT Gateway uncontrolled search path element Vulnerability (ICSA2012601)	Vulnerability - level 3	Vuln
590542	"B and R" Automation SiteManager Multiple Vulnerabilities (ICSA-20-273-03)	Vulnerability - level 3	Vuln
590543	Phoenix Contact Automation Worx Software Suite Multiple Vulnerabilities (ICSA-20-191-01)	Vulnerability - level 3	Vuln
590544	Schneider Electric EcoStruxure and SCADAPack Path Traversal Vulnerability (ICSA-21-259-02)	Vulnerability - level 3	Vuln
590546	JTEKT TOYOPUC Products Denial of Service (DoS) Vulnerability (ICSA-21-245-02)	Vulnerability - level 3	Vuln
590548	JTEKT TOYOPUC PLC Denial of Service (DoS) Vulnerability (ICSA-21-180-04)	Vulnerability - level 3	Vuln
590549	JTEKT TOYOPUC products Denial of Service (DoS) Vulnerability (ICSA-21-103-03)	Vulnerability - level 3	Vuln
590550	Tridium Niagara Multiple Vulnerabilities (ICSA-19-262-01)	Vulnerability - level 3	Vuln
590551	Johnson Controls exacqVision Server Bundle Vulnerability (ICSA-21-280-01)	Vulnerability - level 3	Vuln

590552	Siemens SIMATIC Software Products (Update A) Incorrect Permission Assignment for Critical Resource Vulnerability (ICSA-21-194-06)	Vulnerability - level 3	Vuln
590553	Moxa MXview Network Management Software Multiple Vulnerabilities (ICSA-21-278-03)	Vulnerability - level 3	Vuln
590554	Johnson Controls exacqVision Denial of Service (DoS) Vulnerability (ICSA-21-280-03)	Vulnerability - level 3	Vuln
590555	Schneider Electric CNM Improper Privilege Management Vulnerability (ICSA-21-287-01)	Potential Vulnerability - level 3	Practice
590556	Opto 22 Multiple Product Multiple Vulnerabilities (ICSA-15-120-01)	Vulnerability - level 5	Vuln
590557	Tibbo AggreGate Platform Multiple Vulnerabilities (ICSA-15-323-01)	Vulnerability - level 5	Vuln
590558	GE Digital HMI/SCADA iFIX Multiple Vulnerabilities (ICSA-21-040-01)	Vulnerability - level 1	Vuln
590559	Schneider Electric SoMachine HVAC Multiple Vulnerabilities (ICSA-17-136-02)	Vulnerability - level 3	Vuln
590560	Schneider Electric StruxureOn Gateway Remote Code Execution (RCE) Vulnerability (ICSA-18-046-04)	Vulnerability - level 5	Vuln
590561	GE Common Licensing Multiple Vulnerabilities (GED SecComm 18-02)	Vulnerability - level 4	Vuln
590562	WellinTech KingView Multiple Vulnerabilities (ICSA-12-185-01)	Vulnerability - level 3	Vuln
590563	Siemens SIMATIC WinCC Products (Update B) Multiple Vulnerabilities (ICSA-21-131-12)	Vulnerability - level 3	Vuln
590566	PHOENIX CONTACT FL COMSERVER, FL COM SERVER, and PSI-MODEM/ETH Cross-Site Scripting (XSS) Vulnerability (ICSA-17-341-03)	Vulnerability - level 3	Vuln
590567	PHOENIX CONTACT mGuard Default Password Vulnerability (ICSA-17-017-01)	Vulnerability - level 5	Vuln
590568	PHOENIX CONTACT FL SWITCH Multiple Vulnerabilities (ICSA-18-011-03)	Vulnerability - level 5	Vuln
590569	PHOENIX CONTACT mGuard Multiple Vulnerabilities (ICSA-17-131-01)	Vulnerability - level 3	Vuln
590570	PHOENIX CONTACT Emalytics Controller ILC Incorrect Permission Assignment for Critical Resource Vulnerability (ICSA-20-063-02)	Vulnerability - level 5	Vuln
590571	PHOENIX CONTACT WLAN Capable Devices using the WPA2 Protocol Multiple Vulnerabilities (ICSA-17-325-01)	Potential Vulnerability - level 3	Practice
590572	PHOENIX CONTACT FL SWITCH Multiple Vulnerabilities (ICSA-19-024-02)	Vulnerability - level 5	Vuln
590573	PHOENIX CONTACT RAD-80211-XD Vulnerability (ICSA-19-085-02)	Vulnerability - level 3	Vuln
590574	PHOENIX CONTACT FL SWITCH 3xxx/4xxx/48xx Series Multiple Vulnerabilities (ICSA-18-137-02)	Vulnerability - level 5	Vuln
590575	Siemens SCALANCE Multiple Vulnerabilities (ICSA-21-287-07)	Potential Vulnerability - level 5	Practice
590576	PHOENIX CONTACT PLCNext AXC F 2152 Multiple Vulnerabilities (ICSA-19-155-01)	Potential Vulnerability - level 3	Practice
590577	PHOENIX CONTACT mGuard Improper Validation of Integrity Check Value Vulnerability (ICSA-18-030-01)	Vulnerability - level 3	Vuln
590578	Emerson HART DTM Vulnerability (Update A) Denial of Service (DoS) Vulnerability (ICSA-15-008-01A)	Potential Vulnerability - level 3	Practice
590579	Siemens RUGGEDCOM ROX Devices Denial of Service (DoS) Vulnerability (ICSA-21-287-08)	Vulnerability - level 3	Vuln
590580	Siemens SINUMERIK Heap-based Buffer Overflow Vulnerability (ICSA-21-287-04)	Vulnerability - level 3	Vuln
590581	Siemens SCALANCE W1750D (all versions) Multiple Vulnerabilities (ICSA-21-287-07)	Vulnerability - level 3	Vuln
590582	Emerson WirelessHART Gateway Improper Access Control Vulnerability (ICSA-20-135-02)	Potential Vulnerability - level 5	Practice

590583	Emerson Ovation OCR400 Controller Multiple Vulnerabilities (ICSA-19-148-01)	Potential Vulnerability - level 3	Practice
590584	Emerson ROC800 (Update B) Multiple Vulnerabilities (ICSA-13-259-01B)	Vulnerability - level 3	Vuln
590585	Emerson DeltaV Wireless I/O Card Open SSH Port Vulnerability (ICSA-16-334-03)	Potential Vulnerability - level 3	Practice
590586	Emerson DeltaV Uncontroller Resource Consumption Denial of Service (DoS) Vulnerability (ICSA-13-053-01)	Potential Vulnerability - level 3	Practice
590587	Emerson ControlWave Micro Process Automation Controller Denial of Service (DoS) Vulnerability (ICSA-18-058-03)	Potential Vulnerability - level 3	Practice
590588	AUVESY Versiondog Multiple Vulnerabilities (ICSA-21-292-01)	Vulnerability - level 5	Vuln
590589	AVEVA SuiteLink Server Multiple Vulnerabilities (ICSA-21-231-01)	Vulnerability - level 3	Vuln
590590	AVEVA PCS Portal Uncontrolled Search Path Element Vulnerability (ICSA-21-252-01)	Vulnerability - level 3	Vuln
590591	Siemens SINEC NMS Multiple Vulnerabilities (ICSA-21-287-05)	Vulnerability - level 5	Vuln
590592	Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Update I) Unquoted Search Path or Element Vulnerability (ICSA-20-161-04)	Potential Vulnerability - level 3	Practice
590593	GE Common Licensing Multiple Vulnerabilities (GED SecComm 18-02)	Vulnerability - level 3	Vuln
590594	FATEK Automation Communication Server Stack based Buffer Overflow Vulnerability (ICSA-21-280-07)	Vulnerability - level 3	Vuln
590595	VISAM VBASE Editor Multiple Vulnerabilities (ICSA-21-308-01)	Vulnerability - level 3	Vuln
590597	Omron CX-One Stack based Buffer Overflow Vulnerability (ICSA-21-131-01)	Vulnerability - level 3	Vuln
590598	Mitsubishi Electric MELSEC iQ-R Multiple Vulnerabilities (ICSA-20-303-02)	Potential Vulnerability - level 5	Practice
590599	Mitsubishi Electric MELFA (Update A) Uncontrolled Resource Consumption Vulnerability (ICSA-21-021-04)	Vulnerability - level 3	Vuln
590600	Mitsubishi Electric MELSEC iQ-R Series (Update C) Uncontrolled Resource Consumption Vulnerability (ICSA-20-282-02)	Vulnerability - level 3	Vuln
590601	Mitsubishi Electric Multiple Products (Update C) Predictable Exact Value from Previous Values Vulnerability (ICSA-20-245-01)	Potential Vulnerability - level 4	Practice
590602	Resource Data Management Intuitive 650 TDB Controller (Update A) Multiple Vulnerabilities (ICSA-16-140-01)	Vulnerability - level 5	Vuln
590603	mySCADA myDESIGNER Relative Path Traversal Vulnerability (ICSA-21-313-04)	Vulnerability - level 3	Vuln
590604	OSIsoft PI Web API Cross-Site Scripting (XSS) Vulnerability (ICSA-21-313-06)	Vulnerability - level 3	Vuln
590605	Network Vision IntraVue Code Injection Vulnerability (ICSA-15-057-01)	Vulnerability - level 5	Vuln
590608	Siemens SIMATIC HMI Devices (Update E) Multiple Vulnerabilities (ICSA-15-099-01E)	Potential Vulnerability - level 3	Practice
590609	Mitsubishi Electric FA Engineering Software Products (Update C) Multiple Vulnerabilities (ICSA-21-049-02)	Vulnerability - level 5	Vuln
590610	Mitsubishi Electric MELSEC iQ-F Series Denial of Service (DoS) Vulnerability (ICSA-20-345-01)	Potential Vulnerability - level 3	Practice
590611	Mitsubishi Electric GOT and Tension Controller (Update A) Denial of Service (DoS) Vulnerability (ICSA-20-343-02)	Potential Vulnerability - level 3	Practice
590612	Siemens SENTRON powermanager Incorrect Permission Assignment for Critical Resource Vulnerability (ICSA-21-315-10)	Potential Vulnerability - level 4	Practice
590615	FATEK Automation PLC WinProladder Stack-based Buffer Overflow Vulnerability (ICSA-20-254-02)	Vulnerability - level 3	Vuln
590616	Tridium NiagaraAX Directory Traversal Vulnerability (ICSA-13-045-01)	Vulnerability - level 5	Vuln
590617	Schneider Electric APC Easy UPS On-Line Multiple Vulnerabilities (ICSA-20-224-02)	Vulnerability - level 5	Vuln
590618	ICONICS GENESIS64 Denial of Service (DoS) Vulnerability (ICSA-21-294-03)	Vulnerability - level 3	Vuln

590620	Fuji Electric Tellus Lite V-Simulator and V-Server Lite Multiple Vulnerabilities (ICSA-21-299-01)	Vulnerability - level 4	Vuln
590621	FATEK Automation WinProLadder Multiple Vulnerabilities (ICSA-21-320-01)	Vulnerability - level 4	Vuln
590622	Delta Electronics CNCSoft Arbitrary Code Execution Vulnerability (ICSA-21-334-03)	Vulnerability - level 3	Vuln
590625	AzeoTech DAQFactory Multiple Vulnerabilities (ICSA-21-308-02)	Vulnerability - level 4	Vuln
590626	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L and FX Series CPU Modules (Update A) Uncontrolled Resource Consumption Vulnerability (ICSA-20-175-01)	Vulnerability - level 5	Vuln
590627	Mitsubishi Electric MELSEC Denial of Service (DoS) Vulnerability (ICSA-20-091-02)	Vulnerability - level 3	Vuln
590628	Mitsubishi Electric GOT2000 Series Multiple Vulnerabilities (ICSA-20-189-02)	Potential Vulnerability - level 5	Practice
590629	Mitsubishi Electric MELSEC-Q Series Ethernet Module Denial of Service (DoS) Vulnerability (ICSA-19-141-02)	Vulnerability - level 3	Vuln
590630	Mitsubishi Electric GOT and Tension Controller Multiple Vulnerabilities (ICSA-21-278-01)	Vulnerability - level 3	Vuln
590631	Mitsubishi Electric MELSEC iQ-R Series (Update C) Denial of Service (DoS) Vulnerability (ICSA-20-324-05)	Vulnerability - level 3	Vuln
590632	Mitsubishi Electric MELSEC iQ-R Series (Update C) Denial of Service (DoS) Vulnerability (ICSA-20-161-02)	Vulnerability - level 3	Vuln
590633	Mitsubishi Electric MELSEC iQ-R, Q and L Series (Update A) Denial of Service (DoS) Vulnerability (ICSA-20-303-01)	Vulnerability - level 3	Practice
590634	Mitsubishi Electric MELSEC-Q Series PLCs Denial of Service (DoS) Vulnerability (ICSA-19-029-02)	Vulnerability - level 3	Vuln
590636	Mitsubishi Electric MELSEC-Q Series Ethernet Interface Module Multiple Vulnerabilities (ICSA-16-336-03)	Vulnerability - level 3	Vuln
590639	Siemens RUGGEDCOM Win Transmission Control Protocol (TCP) URGENT/11 Multiple Vulnerabilities (SSA-189842)	Vulnerability - level 4	Vuln
590640	Siemens Power Meters Urgent/11 Transmission Control Protocol/Internet Protocol (TCP/IP) Stack Multiple Vulnerabilities (SSA-352504)	Vulnerability - level 4	Vuln
590641	Siemens SIPROTEC 5 Ethernet plug-in communication modules and devices Multiple Vulnerabilities (SSA-632562)	Potential Vulnerability - level 4	Practice
590644	3S-Smart CODESYS GmbH v3 (Update A) Vulnerability (ICSA-19-213-04)	Vulnerability - level 3	Vuln
590645	3S-Smart CODESYS GmbH v3 Web Server Multiple Vulnerabilities (ICSA-19-255-01)	Vulnerability - level 4	Vuln
590647	Mitsubishi Electric MELSEC iQ-R Series Multiple Vulnerabilities (ICSA-21-250-01)	Vulnerability - level 5	Vuln
590648	Mitsubishi Electric GT14 Model of GOT1000 Series Multiple Vulnerabilities (ICSA-20-310-02)	Potential Vulnerability - level 4	Practice
590649	Mitsubishi Electric MELSEC and MELIPC Series Multiple Vulnerabilities (ICSA-21-334-02)	Potential Vulnerability - level 4	Practice
590650	Mitsubishi Electric MELSEC iQ-R Series Authorization Bypass Through User-controlled Key Vulnerability (ICSA-21-287-03)	Vulnerability - level 4	Vuln
590651	Mitsubishi Electric MELSEC iQ-R Series C Controller Module (Update A) Denial of Service (DoS) Vulnerability (ICSA-21-280-04)	Vulnerability - level 3	Vuln
590652	Mitsubishi Electric MELSEC iQ-R Series Denial of Service (DoS) Vulnerability (ICSA-21-147-05)	Vulnerability - level 4	Vuln
590654	Mitsubishi Electric MELSEC-F Series Denial of Service (DoS) Vulnerability (ICSA-21-201-01)	Vulnerability - level 4	Vuln
590657	Mitsubishi Electric FA Engineering Software Multiple Vulnerabilities (ICSA-21-350-05)	Vulnerability - level 2	Vuln
590658	Wibu-Systems CodeMeter Runtime Vulnerability (ICSA-21-350-03)	Potential Vulnerability - level 2	Practice
590659	Advantech WebAccess SCADA Information Disclosure Vulnerability (ICSA-21-285-01)	Vulnerability - level 2	Vuln

590660	Siemens SINEC NMS Multiple Vulnerabilities (ICSA-21-257-14)	Vulnerability - level 3	Vuln
590665	3S-Smart CODESYS GmbH v3 Multiple Vulnerabilities (ICSA-19-213-03)	Vulnerability - level 4	Vuln
590667	Schneider Electric NMC cards and Embedded Devices Multiple Vulnerabilities (ICSA-21-313-01)	Vulnerability - level 3	Vuln
590668	Siemens SIMATIC ITC Multiple Vulnerabilities (ICSA-21-350-12)	Vulnerability - level 4	Vuln
590669	Siemens SCALANCE and RUGGEDCOM Devices SSH (Update A) Vulnerability (ICSA-21-068-02)	Potential Vulnerability - level 3	Practice
590670	Siemens SCALANCE and RUGGEDCOM Devices (Update A) Vulnerability (ICSA-21-068-03)	Vulnerability - level 3	Vuln
590671	Siemens LOGO! 8 BM Denial of Service (DoS) Vulnerability (ICSA-21-068-05)	Vulnerability - level 3	Vuln
590672	Siemens Transmission Control Protocol (TCP) Stack SIMATIC MV400 Multiple Vulnerabilities (ICSA-21-068-07)	Vulnerability - level 3	Vuln
590674	Siemens Web Server of SCALANCE X200 (Update A) Multiple Vulnerabilities (ICSA-21-103-07)	Vulnerability - level 4	Vuln
590675	Siemens SIMATIC S7-1500 Multiple Vulnerabilities (ICSA-21-131-15)	Vulnerability - level 4	Vuln
590676	Siemens SCALANCE W1750D (Update B) Multiple Vulnerabilities (ICSA-21-131-14)	Vulnerability - level 5	Vuln
590677	Siemens SCALANCE XM-400 and XR-500 Devices Vulnerability (ICSA-21-131-10)	Potential Vulnerability - level 4	Practice
590678	Siemens SIMATIC NET CP343-1 Denial of Service (DoS) Vulnerability (ICSA-21-131-07)	Vulnerability - level 4	Vuln
590682	Opto 22 PAC Control Basic Remote Code Execution (RCE) Vulnerability (ICSA-18-247-01)	Vulnerability - level 4	Vuln
590683	Schneider Electric IGSS Data Server Multiple Vulnerabilities (ICSA-22-046-01)	Vulnerability - level 4	Vuln
590684	Advantech WebAccess HMI Designer Multiple Vulnerabilities (ICSA-21-173-01)	Vulnerability - level 4	Vuln
590685	Mitsubishi Electric GOT and Tension Controller (Update B) Denial of Service (DoS) Vulnerability (ICSA-20-343-02)	Vulnerability - level 3	Vuln
590687	Siemens Simcenter STAR-CCM+ Viewer Out-of-bounds Write Vulnerability (ICSA-21-350-15,SSA-161331)	Vulnerability - level 4	Vuln
590688	Siemens Nucleus RTOS-based APOGEE and TALON Products (Update A) Multiple Vulnerabilities (ICSA-21-315-07)	Vulnerability - level 4	Vuln
590690	Siemens Climatix POL909 Vulnerability (ICSA-21-315-09)	Vulnerability - level 4	Vuln
590691	Siemens APOGEE and TALON Vulnerability (ICSA-21-257-07)	Vulnerability - level 5	Vuln
590694	Siemens LOGO! CMR and SIMATIC RTU 3000 (Update A) Vulnerability (ICSA-21-257-13)	Vulnerability - level 2	Vuln
590695	Siemens SIPROTEC 5 (Update A) Vulnerability (ICSA-21-257-16)	Vulnerability - level 3	Vuln
590697	Siemens SINAMICS PERFECT HARMONY GH180 (Update A) Vulnerability (ICSA-21-194-13)	Potential Vulnerability - level 5	Practice
590698	Siemens RWG Universal Controllers Vulnerability (ICSA-21-194-14)	Vulnerability - level 2	Vuln
590699	Siemens TIM 1531 IRC Vulnerability (ICSA-21-159-08)	Vulnerability - level 3	Vuln
590700	Siemens SIMATIC RFID Vulnerability (ICSA-21-159-13)	Vulnerability - level 4	Vuln
590701	Siemens SINAMICS Medium Voltage Products Remote Access (Update B) Multiple Vulnerabilities (ICSA-21-131-04) (ssa-286838)	Potential Vulnerability - level 5	Practice
590702	Siemens SINAMICS Medium Voltage Products Telnet (Update A) Vulnerability (ICSA-21-131-13)	Vulnerability - level 5	Vuln
590705	Siemens Energy PLUSCONTROL 1st Gen Vulnerability (ICSA-21-068-08)	Potential Vulnerability - level 3	Practice
590706	Siemens TCP/IP Stack AMNESIA:33 in SENTRON PAC/3VA Devices (Update C) Multiple Vulnerabilities (ICSA-21-068-06)	Vulnerability - level 4	Vuln
590707	Siemens SIMOTICS, Desigo, APOGEE, and TALON (Update B) Vulnerability (ICSA-20-105-06)	Vulnerability - level 4	Vuln
590708	Mitsubishi Electric Air Conditioning System Vulnerability (ICSA-21-182-04)	Vulnerability - level 3	Vuln

590709	Mitsubishi Electric Air Conditioning Systems Vulnerability (ICSA-21-182-05)	Vulnerability - level 5	Vuln
590710	Mitsubishi Electric GOT (Update A) Vulnerability (ICSA-21-112-02)	Vulnerability - level 3	Vuln
590713	Siemens SIPROTEC 5 relays (Update A) Multiple Vulnerabilities (ICSA-21-257-10)	Potential Vulnerability - level 5	Practice
590714	Siemens POWER METER SICAM Q100 Vulnerability (ICSA-21-350-07)	Vulnerability - level 5	Vuln
590715	Siemens SCALANCE W1750D Multiple Vulnerabilities (ICSA-21-315-06)	Vulnerability - level 5	Vuln
590716	Siemens SIMATIC CP Vulnerability (ICSA-21-257-06, SSA-535997)	Vulnerability - level 2	Vuln
590717	Siemens LOGO! CMR and SIMATIC RTU 3000 Multiple Vulnerabilities (ICSA-21-257-20)	Vulnerability - level 3	Vuln
590718	3S-Smart CODESYS GmbH Control v3 Products Vulnerability (ICSA-18-352-03)	Vulnerability - level 5	Vuln
590719	Schneider Electric PLC Simulator on EcoStruxure Control Expert and Process Expert Multiple Vulnerabilities (SEVD-2020-315-07)	Potential Vulnerability - level 5	Practice
590720	Siemens SIMOTICS CONNECT 400 Multiple Vulnerabilities (ICSA-21-103-13)	Vulnerability - level 3	Vuln
590721	Siemens TIM 4R-IE Devices Multiple Vulnerabilities (ICSA-21-103-11)	Vulnerability - level 4	Vuln
590723	Schneider Electric Floating License Manager for CitectSCADA, CitectHistorian and Citect Anywhere Multiple Vulnerabilities (ICSA-18-144-01)	Vulnerability - level 5	Vuln
590724	Mitsubishi Electric GOT and Tension Controller (Update A) Vulnerability (ICSA-21-131-02)	Vulnerability - level 3	Vuln
590727	WIBU CodeMeter PASVisu Multiple Vulnerabilities	Vulnerability - level 4	Vuln
590729	Rockwell Automation ISaGRAF5 Runtime Multiple Vulnerabilities (ICSA-20-280-01)	Vulnerability - level 5	Vuln
590730	Siemens JT2Go Multiple Vulnerabilities (ICSA-21-350-10)	Vulnerability - level 4	Vuln
590734	WIBU Codemeter Runtime PAS4000 Multiple Vulnerabilities (adv_1005485-de-02)	Vulnerability - level 4	Vuln
590736	Siemens SIMATIC NET CP 443-1 OPC UA Multiple Vulnerabilities (ICSA-21-159-11)	Potential Vulnerability - level 5	Practice
590739	Siemens SIMATIC S7-1200 Improper Authentication Vulnerability (ICSA-21-222-09)	Potential Vulnerability - level 3	Practice
590740	Siemens SIMATIC NET CP Modules Vulnerability (ICSA-21-257-15)	Potential Vulnerability - level 4	Practice
590741	Siemens RUGGEDCOM ROX Multiple Vulnerabilities (ICSA-21-259-01)	Vulnerability - level 4	Vuln
590746	Siemens Nucleus RTOS Transmission Control Protocol/Internet Protocol (TCP/IP) Stack Multiple Vulnerabilities (SSA-114589)	Vulnerability - level 5	Vuln
590748	Siemens SIMATIC WinCC and PCS Multiple Vulnerabilities (ICSA-22-041-02)	Vulnerability - level 2	Vuln
590749	Rockwell Automation MicroLogix 1100 Vulnerability (ICSA-21-189-01)	Vulnerability - level 4	Vuln
590750	Johnson Controls Sensormatic Electronics KT-1 Vulnerability (ICSA-21-257-02) (JCI-PSA-2021-14)	Vulnerability - level 4	Vuln
590754	3S-Smart CODESYS GmbH Denial of Service (DoS) Vulnerability (Advisory2021-07)	Vulnerability - level 5	Vuln
590755	Siemens SIMATIC CP 1543-1 Multiple Vulnerabilities (SSA-672373)	Vulnerability - level 3	Vuln
590756	ProSoft Technology ICX35 Vulnerability (ICSA-21-056-04)	Vulnerability - level 4	Vuln
590757	Rockwell Automation Micro800 and MicroLogix 1400 Vulnerability (ICSA-21-145-02)	Potential Vulnerability - level 4	Practice
590758	Siemens VxWorks-based Industrial Products Vulnerability (ICSA-21-194-12) (SSA-560465)	Vulnerability - level 5	Vuln
590760	Siemens SIMATIC NET CP Multiple Vulnerabilities (ICSA-21-222-07)	Vulnerability - level 4	Vuln
590762	FATEK Automation FvDesigner Multiple Vulnerabilities (ICSA-22-055-01)	Vulnerability - level 4	Vuln

590764	Mitsubishi Electric EcoWebServerIII Multiple Vulnerabilities (ICSA-22-055-02)	Vulnerability - level 4	Vuln
590766	Schneider Electric Modicon Controllers and SCADAPack RTU Vulnerability (SEVD-2017-065-01)	Potential Vulnerability - level 5	Practice
590781	Rockwell Automation AADvance Controller and Micro800 family Multiple Vulnerabilities (ICSA-20-280-01)	Vulnerability - level 5	Vuln
590785	Schneider Electric Lexium ILE ILA ILS and Altivar Multiple Vulnerabilities (SEVD-2021-217-01)	Vulnerability - level 5	Vuln
590789	Schneider Electric Sepam ACE850 Treck Hypertext Transfer Protocol Server (HTTP Server) Vulnerability (SEVD-2021-012-03)	Vulnerability - level 5	Vuln
590790	Siemens Solid Edge and JT2Go Multiple Vulnerabilities (ICSA-22-041-07)	Potential Vulnerability - level 4	Practice
590791	Delta Electronics DOPSoft (Update A) Vulnerability (ICSA-21-238-04)	Vulnerability - level 3	Vuln
590792	Siemens Energy PLUSCONTROL 1st Gen Devices Multiple Vulnerabilities (SSA-845392)	Vulnerability - level 4	Vuln
590793	WECON PLC Editor Multiple Vulnerabilities (ICSA-21-315-01)	Vulnerability - level 3	Vuln
590794	TURCK BL20 and BL67 Programmable Gateway Hard-Coded User Accounts Vulnerability (ICSA-13-136-01)	Vulnerability - level 5	Vuln
590795	Siemens SIMOTICS CONNECT 400 Multiple Vulnerabilities (ICSA-22-069-02) (SSA-223353)	Vulnerability - level 5	Vuln
590796	Siemens PROFINET Devices (Update C) Vulnerability (ICSA-21-194-03)	Vulnerability - level 4	Vuln
590797	Mitsubishi Electric GX Works2 Denial of Service (DoS) Vulnerability (ICSA-21-350-04)	Vulnerability - level 4	Vuln
590798	Delta Electronics CNCSoft Multiple Vulnerabilities (ICSA-21-350-02)	Vulnerability - level 3	Vuln
590799	Delta Electronics DOPSoft 2 Multiple Vulnerabilities (ICSA-21-252-02)	Vulnerability - level 4	Vuln
590800	Siemens SICAM PQ Analyzer Denial of Service (DoS) Vulnerability (ICSA-22-013-06)	Vulnerability - level 4	Vuln
590801	Siemens Simcenter Femap Multiple Vulnerabilities (ICSA-22-069-10,SSA-94918)	Vulnerability - level 4	Vuln
590803	Siemens SICAM A8000 Multiple Vulnerabilities (SSA-324998)	Vulnerability - level 4	Vuln
590804	Schneider Electric Easergy P3 Vulnerability (SEVD-2022-011-04)	Vulnerability - level 4	Vuln
590805	Siemens SINEC NMS Multiple Vulnerabilities (ICSA-22-069-03,SSA-250085)	Vulnerability - level 4	Vuln
590806	Schneider Electric Easergy P5 Multiple Vulnerabilities (SEVD-2022-011-03)	Vulnerability - level 4	Vuln
590807	Siemens Simcenter STAR-CCM+ Viewer Multiple Vulnerabilities (ICSA-22-069-05,SSA-166747)	Vulnerability - level 4	Vuln
590809	GE Proficy CIMPLICITY-IPM Multiple Vulnerabilities (ICSA-22-053-01)	Vulnerability - level 4	Vuln
590810	Rockwell Automation Studio 5000 Logix Designer Vulnerability (ICSA-22-090-07)	Vulnerability - level 4	Vuln
590811	Rockwell Automation Logix Controllers Vulnerability (ICSA-22-090-05)	Potential Vulnerability - level 5	Practice
590817	Schneider Electric Treck HTTP Server Vulnerability on TM3 Bus Coupler Modules Vulnerability (SEVD-2020-353-02)	Vulnerability - level 5	Vuln
590818	Schneider Electric CODESYS v2 Vulnerabilities in Programmable Automation Controller (PacDrive) M Multiple Vulnerabilities (SEVD-2021-222-06)	Vulnerability - level 5	Vuln
590819	Schneider Electric Treck TCP/IP Multiple Vulnerabilities (SEVD-2020-175-01)	Potential Vulnerability - level 5	Practice
590821	WAGO NUCLEUS Transmission Control Protocol (TCP) Stack Multiple Vulnerabilities (VDE-2021-050)	Vulnerability - level 5	Vuln
590822	Siemens SIMATIC WinCC (Update B) Multiple Vulnerabilities (ICSA-21-315-03)	Vulnerability - level 5	Vuln

590835	Inductive Automation Ignition Code Execution Vulnerability (ICSA-22-102-03)	Vulnerability - level 3	Vuln
590837	Schneider Electric Pelco VideoXpert Enterprise Multiple Vulnerabilities (ICSA-17-355-02)	Vulnerability - level 4	Vuln
590843	Advantech WebAccess Multiple Vulnerabilities (ICSA-18-298-02)	Vulnerability - level 4	Vuln
590844	Advantech WebAccess Multiple Vulnerabilities (ICSA-18-296-01)	Vulnerability - level 5	Vuln
590849	ABB OPC Server for AC 800M Remote Code Execution (RCE) Vulnerability (ICSA-22-074-01)	Vulnerability - level 4	Vuln
590852	Siemens ProcessSuite and Invensys Intouch Poorly Encrypted Password File Vulnerability (ICSA-12-348-01)	Potential Vulnerability - level 3	Practice
590853	Siemens SIMATIC S7-400 Vulnerability (icsa-22-104-12) (ssa-557541)	Vulnerability - level 4	Vuln
590854	Schneider Electric TelevisGo Multiple Vulnerabilities (SEVD-2019-225-05)	Potential Vulnerability - level 5	Practice
590855	Delta Electronics DOPSoft (Update A) Multiple Vulnerabilities (ICSA-21-182-03)	Vulnerability - level 4	Vuln
590856	Fuji Electric Alpha5 Multiple Vulnerabilities (ICSA-22-090-03)	Vulnerability - level 4	Vuln
590857	AVEVA InTouch Access Anywhere and Plant SCADA Access Anywhere Vulnerability (ICSA-22-130-05)	Vulnerability - level 5	Vuln
590859	Fuji Electric Energy Savings Estimator Vulnerability (ICSA-18-282-07)	Vulnerability - level 4	Vuln
590865	Mitsubishi Electric MELSEC-Q Series C Controller Module Vulnerability (ICSA-22-102-02) (2022-001)	Potential Vulnerability - level 5	Practice
590867	Measuresoft ScadaPro DLL Hijack Vulnerability (ICSA-12-145-01)	Vulnerability - level 3	Vuln
590868	Yokogawa CENTUM Multiple Vulnerabilities (ICSA-22-083-01) (YSAR-22-0001)	Vulnerability - level 5	Vuln
590869	Panasonic FPWIN Pro Multiple Vulnerabilities (ICSA-16-131-01)	Vulnerability - level 3	Vuln
590870	Mitsubishi Electric MELSOFT iQ AppPortal Multiple Vulnerabilities (ICSA-22-132-02)	Potential Vulnerability - level 5	Practice
590871	Siemens SCALANCE W1700 Multiple Vulnerabilities (ICSA-22-104-08) (SSA-392912)	Vulnerability - level 4	Vuln
590873	Honeywell Experion PKS and ACE Controllers Multiple Vulnerabilities (ICSA-21-278-04) (SN 2021-02-22 01)	Vulnerability - level 3	Vuln
590874	ABB SPIET800 and PNI800 Multiple Vulnerabilities (ICSA-22-097-02)	Potential Vulnerability - level 4	Practice
590877	Fultek WinTr Directory Traversal Vulnerability (ICSA-12-262-01)	Vulnerability - level 4	Vuln
590878	Schneider Electric Wibu-Systems CodeMeter Multiple Vulnerabilities (SEVD-2020-287-02)	Vulnerability - level 5	Vuln
590879	Rockwell Automation Stratix Switches Impacted by IOS and IOS XE Software Multiple Vulnerabilities (PN1558)	Vulnerability - level 4	Practice
590880	Schneider Electric Wonderware System Platform Arbitrary Code Execution Vulnerability (ICSA-15-169-02)	Vulnerability - level 3	Vuln
590882	Schneider Electric InduSoft Web Studio and InTouch Machine Edition 2014 Password Storage Multiple Vulnerabilities (ICSA-15-211-01)	Vulnerability - level 4	Vuln
590883	Mitsubishi Electric MELSEC-Q/L Series Ethernet Interface Module and MELSEC iQ-R Series MES Interface Module Vulnerability (2022-006)	Vulnerability - level 4	Vuln
590894	Mitsubishi Electric GOT products Vulnerability (ICSA-21-320-02) (2021-018)	Vulnerability - level 4	Vuln
590901	Horner Automation Cscape Csfont Multiple Vulnerabilities (ICSA-22-146-02)	Vulnerability - level 4	Vuln
590902	Elcomplus SmartPTT SCADA Multiple Vulnerabilities (ICSA-22-109-04)	Vulnerability - level 5	Vuln
590904	Moxa NPort IAW5000A-I/O Series Serial Device Server Multiple Vulnerabilities (ICSA-21-187-01)	Vulnerability - level 5	Vuln
590907	Schneider Electric Embedded FTP Servers for Modicon PAC Controllers Multiple Vulnerabilities (SEVD-2018-081-01)	Vulnerability - level 5	Vuln

590909	Hitachi Energy Relion 670/650/SAM600-IO Vulnerability (ICSA-21-336-05)	Vulnerability - level 4	Vuln
590910	Ocean Data Systems Dream Reports Cross-Site Scripting (XSS) and Write Access Violation Multiple Vulnerabilities (ICSA-12-024-01)	Vulnerability - level 5	Vuln
590911	Siemens SIMATIC CP 44x-1 RNA Vulnerability (ICSA-22-132-11) (SSA-480937)	Vulnerability - level 3	Vuln
590913	Mitsubishi Electric MELSEC Q and L Series Ethernet Port Denial of Service (DoS) Vulnerability (2022-007) (ICSA-22-172-01)	Potential Vulnerability - level 4	Practice
590914	Rockwell Automation Logix Controllers Vulnerability (ICSA-22-144-01) (PN1596)	Vulnerability - level 3	Vuln
590916	PHOENIX CONTACT mGuard Device Manager Multiple Vulnerabilities (ICSA-17-262-01)	Vulnerability - level 5	Vuln
590917	Mitsubishi Electric FA Products (Update A) Multiple Vulnerabilities (ICSA-22-090-04)	Vulnerability - level 5	Vuln
590919	Johnson Controls Facility Explorer Multiple Vulnerabilities (JCI-PSA-2019-10 v1)	Vulnerability - level 4	Vuln
590927	GEOVAP Reliance 4 SCADA/HMI Vulnerability (ICSA-18-298-01)	Vulnerability - level 3	Vuln
590928	Carrier LenelS2 HID Mercury access panels Multiple Vulnerabilities (ICSA-22-153-01)	Potential Vulnerability - level 5	Practice
590931	Schneider Electric Modicon M340 Controller Vulnerability (SEVD-2019-225-02)	Potential Vulnerability - level 4	Practice
590934	Rockwell Automation MicroLogix Vulnerability (ICSA-22-188-01) (PN1597)	Vulnerability - level 3	Vuln
590937	Siemens SIMATIC WinAC RTX (F) 2010 Multiple Vulnerabilities (ssa-608355)	Potential Vulnerability - level 3	Practice
590941	Siemens SCALANCE X-200 Web Hijack Vulnerability Vulnerability (SSA-850708) (ICSA-13-254-01)	Vulnerability - level 3	Vuln
590942	Siemens SIMATIC S7-1200 CPU Protection Mechanism Failure Vulnerability (SSA-833048) (ICSA-16-075-01)	Vulnerability - level 3	Vuln
590943	General Electric D20MX (Update A) Multiple Vulnerabilities (ICSA-13-091-01)	Vulnerability - level 5	Vuln
590944	Schneider Electric Easergy P5 and P3 (Update A) Multiple Vulnerabilities (ICSA-22-055-03)	Vulnerability - level 4	Vuln
590945	ABB REB500 WindRiver VxWorks IPNet Multiple Vulnerabilities (ABBVU-PGGA-REB500-1KHL501885)	Vulnerability - level 5	Vuln
590946	Siemens Mendix Improper Access Control Vulnerability (ICSA-22-104-17)	Vulnerability - level 3	Vuln
590948	Advantech Spectre RT Industrial Routers Multiple Vulnerabilities (ICSA-21-054-03)	Vulnerability - level 5	Vuln
590949	General Electric Renewable Energy MDS Radios Multiple Vulnerabilities (ICSA-22-090-06)	Vulnerability - level 4	Vuln
590955	JTEKT TOYOPUC Multiple Vulnerabilities (ICSA-22-172-02)	Vulnerability - level 4	Vuln
590957	Johnson Controls Exacq Technologies exacqVision Vulnerability (ICSA-21-077-01)	Vulnerability - level 3	Vuln
590958	Advantech BB-ESWGP506-2SFP-T Vulnerability (ICSA-21-054-02)	Vulnerability - level 5	Vuln
590960	Siemens EN100 Ethernet Module Vulnerability (ICSA-22-167-05) (SSA-693555)	Potential Vulnerability - level 4	Practice
590962	Siemens SIMATIC MV500 Devices Multiple Vulnerabilities (ICSA-22-195-03) (SSA-348662)	Vulnerability - level 4	Vuln
590963	PerFact Open Virtual Private Network (OpenVPN) Client Multiple Vulnerabilities (ICSA-21-056-01)	Vulnerability - level 4	Vuln
590965	Schneider Electric Easergy P5 Multiple Vulnerabilities (SEVD-2022-193-04)	Vulnerability - level 5	Vuln
590967	Siemens SICAM P850 and SICAM P855 Multiple Vulnerabilities (ICSA-22-132-07) (SSA-165073)	Vulnerability - level 5	Vuln
590968	Siemens Desigo PXC and DXR Devices (Update A) Multiple Vulnerabilities (ICSA-22-132-10) (ssa-662649) (ssa-626968)	Potential Vulnerability - level 5	Practice
590970	Hitachi Energy RTU500 OpenLDAP Multiple Vulnerabilities (ICSA-21-341-01)	Vulnerability - level 4	Vuln

590971	InHand Networks IR615 Router (Update A) Multiple Vulnerabilities (ICSA-21-280-05)	Potential Vulnerability - level 5	Practice
590972	Red Lion DA50N Multiple Vulnerabilities (ICSA-22-104-03)	Potential Vulnerability - level 5	Practice
590975	Delta Electronics CNCSoft-B Multiple Vulnerabilities (ICSA-21-110-05)	Vulnerability - level 4	Vuln
590976	Siemens SCALANCE LPE9403 Third-Party Multiple Vulnerabilities (ICSA-22-167-09) (SSA-222547)	Vulnerability - level 5	Vuln
590978	Siemens RUGGEDCOM ROX Vulnerability (ICSA-22-195-05) (SSA-599506)	Vulnerability - level 4	Vuln
590979	MOXA NPort 5110 Multiple Vulnerabilities (ICSA-22-207-04)	Vulnerability - level 4	Vuln
590980	Siemens SCALANCE X Switch Devices Multiple Vulnerabilities (ICSA-22-195-01)	Vulnerability - level 5	Vuln
590983	Siemens JT2GO Multiple Vulnerabilities (ICSA-22-132-09)	Vulnerability - level 4	Vuln
590984	Siemens Simcenter Femap Out-of-bounds Write Vulnerability (ICSA-22-132-14)	Vulnerability - level 4	Vuln
590985	ABB e-Design Multiple Vulnerabilities (ICSA-22-179-01)	Vulnerability - level 4	Vuln
590987	AutomationDirect C-More EA9 HMI Multiple Vulnerabilities (ICSA-22-167-01)	Vulnerability - level 4	Vuln
590990	Delta Electronics CNCSoft Multiple Vulnerabilities (ICSA-22-132-01)	Vulnerability - level 4	Vuln
590992	Siemens S7-1200 Web Application Cross-Site Scripting (XSS) Vulnerability (ICSA-12-283-01) (SSA-279823)	Vulnerability - level 4	Vuln
590996	Hitachi ABB Power Grids Relion 670/650 series Relion SAM600-IO Multiple Vulnerabilities (1MRG035816)	Vulnerability - level 5	Vuln
591000	Inductive Automation Ignition (Update A) Vulnerability (ICSA-22-207-01)	Vulnerability - level 5	Vuln
591001	Delta Electronics DIAEnergie (Update C) Multiple Vulnerabilities (ICSA-22-081-01)	Vulnerability - level 5	Vuln
591003	SIMPLight SCADA Software Uncontrolled Search Path Element Vulnerability (ICSA-17-222-01)	Vulnerability - level 4	Vuln
591004	ABB NSD570 Multiple Vulnerabilities (ABBVU-PGGA-NSD570-1KHW003577)	Vulnerability - level 5	Vuln
591005	Johnson Controls Facility Explorer Vulnerability (ICSA-21-182-01)	Vulnerability - level 4	Vuln
591006	Delta Electronics DIALink Multiple Vulnerabilities (ICSA-21-294-02)	Vulnerability - level 4	Vuln
591007	Siemens SIMATIC NMS and SINAMICS Stardrive (Update J) Multiple Vulnerabilities (ICSA-20-161-04)	Vulnerability - level 3	Vuln
591008	ABB Drive Composer, Automation Builder, Mint Workbench Multiple Vulnerabilities (ICSA-22-202-01) (ABBVREP0072)	Vulnerability - level 4	Vuln
591010	ABB RTU500 series Multiple Vulnerabilities (ABBVU-PGGA-RTU500-1KGT090327)	Vulnerability - level 5	Vuln
591018	Hitachi Energy RTU500 series Multiple Vulnerabilities (ICSA-21-336-08)	Vulnerability - level 4	Vuln
591021	Siemens SIMATIC S7-400 PN CPU Denial of Service (DoS) Vulnerability (ssa-589272) (ICSA-12-212-02)	Vulnerability - level 4	Vuln
591025	Siemens SIMATIC S7-1200 Improper Input Validation Multiple Vulnerabilities (SSA-724606) (ICSA-14-079-01)	Vulnerability - level 4	Vuln
591031	Siemens SCALANCE XM-400 and XR-500 Vulnerability (SSA-145224) (ICSA-22-167-10)	Vulnerability - level 4	Vuln
591032	Siemens TIM 1531 IRC Vulnerability (ICSA-18-088-02) (SSA-110922)	Vulnerability - level 5	Vuln
591034	Siemens SCALANCE X-300 Switches Multiple Vulnerabilities (SSA-836527) (ICSA-22-104-09)	Vulnerability - level 5	Vuln
591035	Siemens SCALANCE FragAttacks Multiple Vulnerabilities (ICSA-22-104-04) (SSA-913875)	Vulnerability - level 3	Vuln
591041	Siemens SIPROTEC 5 Information Disclosure Vulnerability (SSA-439673)	Vulnerability - level 4	Vuln

591050	Siemens SIMATIC WinCC Vulnerability (SSA-363107) (icsa-22-132-06)	Vulnerability - level 4	Vuln
591052	Mitsubishi Electric GENESIS64 Multiple Vulnerabilities (ICSA-22-202-04) (2022-008)	Vulnerability - level 5	Vuln
591053	Rockwell Automation ISaGRAF Workbench Multiple Vulnerabilities (ICSA-22-202-03)	Vulnerability - level 4	Vuln
591054	Mitsubishi Electric MELSOFT GT OPC UA, GT SoftGOT2000 Multiple Vulnerabilities (ICSA-22-130-06)	Vulnerability - level 4	Vuln
591057	Phoenix Contact mGuard devices Vulnerability (Security Advisory 2015/07/14-001)	Vulnerability - level 3	Vuln
591059	Emerson Proficy Machine Edition Multiple Vulnerabilities (ICSA-22-228-06)	Vulnerability - level 4	Vuln
591060	Rockwell Automation ISaGRAF, CCW, SIS Workstation Vulnerability (ICSA-22-088-01) (PN1588)	Vulnerability - level 3	Vuln
591061	Eaton Intelligent Power Manager Vulnerability (ICSA-22-130-04) (ETN-VA-2021-1001a)	Vulnerability - level 3	Vuln
591062	Reolink P2P Cameras Multiple Vulnerabilities (icsa-21-019-02)	Potential Vulnerability - level 4	Practice
591063	Siemens OZW Web Server Vulnerability (ICSA-20-042-09) (SSA-986695)	Vulnerability - level 4	Vuln
591064	Siemens SIMATIC CP 44x-1 Redundant Network Access Modules Vulnerability (ICSA-17-173-01) (SSA-126840)	Potential Vulnerability - level 4	Practice
591067	Emerson ROC800, ROC800L and DL8000 Vulnerability (ICSA-22-223-04)	Potential Vulnerability - level 5	Practice
591068	Rockwell Automation Products INFRA:HALT Interniche Multiple Vulnerabilities (PN1575)	Potential Vulnerability - level 5	Practice
591069	Phoenix Contact Innominate mGuard devices Vulnerability (Security Advisory 2014/12/17-001)	Vulnerability - level 4	Vuln
591071	Siemens SIMATIC S7-1200 CPU Web Multiple Vulnerabilities (ICSA-14-114-02) (SSA-892012)	Vulnerability - level 3	Vuln
591073	Siemens SIMATIC RF350M and SIMATIC RF650M KRACK Attacks Multiple Vulnerabilities (SSA-418456)	Potential Vulnerability - level 3	Practice
591074	Cassia Networks Access Controller Vulnerability (ICSA-21-119-02)	Vulnerability - level 3	Vuln
591076	Resource Data Management Data Manager Privilege Escalation Vulnerability (ICSA-15-265-01)	Vulnerability - level 4	Vuln
591077	Elipse Software Elipse E3 Process Control Vulnerability (ICSA-15-069-04A)	Vulnerability - level 4	Vuln
591081	Siemens SIMATIC CP Devices Multiple Vulnerabilities (SSA-517377) (ICSA-22-195-12)	Vulnerability - level 5	Vuln
591082	Siemens SIMATIC eaSie Multiple Vulnerabilities (SSA-580125) (ICSA-22-195-15)	Vulnerability - level 5	Vuln
591083	"B and R" Industrial Automation Studio 4 Multiple Vulnerabilities (icsa-22-228-05)	Vulnerability - level 5	Vuln
591084	Measuresoft ScadaPro Server Vulnerability (ICSA-22-235-05)	Vulnerability - level 4	Vuln
591085	Siemens SIMATIC S7-1500 CPU Multiple Vulnerabilities (ICSA-16-040-02) (SSA-253230)	Vulnerability - level 4	Vuln
591086	WIBU Systems CodeMeter Runtime Denial of Service (DoS) Vulnerability (WIBU-210910-01)	Potential Vulnerability - level 4	Practice
591092	Delta Electronics Delta Industrial Automation DIALink Multiple Vulnerabilities (ICSA-22-235-02)	Vulnerability - level 4	Vuln
591093	ABB Relion 650, Relion 670 Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (ABB-VU-PGGA-1MRG024369) (ABB-VU-PGGA-1MRG025160)	Vulnerability - level 5	Vuln
591094	Delta Electronics DIAEnergie (Update C) Multiple Vulnerabilities (ICSA-21-238-03)	Vulnerability - level 5	Vuln
591099	Omron SYSMAC CS/CJ/CP Series and NJ/NX Series Multiple Vulnerabilities (icsa-22-179-02)	Potential Vulnerability - level 5	Practice
591100	Siemens JT2Go (ODA) Open Design Alliance Drawings Software Development Kit (SDK) Multiple Vulnerabilities (SSA-429204)	Vulnerability - level 4	Vuln

591102	Honeywell ControlEdge Vulnerability (ICSA-22-242-06)	Vulnerability - level 5	Vuln
591103	Hitachi Energy RTU500 Vulnerability (ICSA-22-235-07)	Vulnerability - level 3	Vuln
591104	Mitsubishi Electric GT25-WLAN (Update A) Multiple Vulnerabilities (ICSA-22-102-04)	Vulnerability - level 3	Vuln
591106	Siemens Simcenter Femap File Parsing Multiple Vulnerabilities (SSA-518824) (icsa-22-258-02)	Vulnerability - level 4	Vuln
591107	Measuresoft ScadaPro Server and Client Multiple Vulnerabilities (ICSA-22-235-06)	Vulnerability - level 4	Vuln
591108	Siemens Simcenter Femap File Parsing Vulnerability (ssa-243317) (icsa-22-195-09)	Vulnerability - level 4	Vuln
591109	Schneider Electric EcoStruxure Power Build: Rapsody Software Multiple Vulnerabilities (SEVD-2021-012-02 V2.0)	Vulnerability - level 3	Vuln
591110	Siemens SIMATIC S7-1200 Multiple Vulnerabilities (ICSA-14-079-02, SSA-654382)	Vulnerability - level 4	Vuln
591115	ABB Relion 670 series and Relion 650 series Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (ABBVU-PGGA-1MRG032388)	Vulnerability - level 4	Vuln
591118	Siemens SIMATIC S7-1500 CPU family Multiple Vulnerabilities (ICSA-14-073-01,SSA-456423)	Potential Vulnerability - level 4	Practice
591119	Siemens LOGO! CMR Family and SIMATIC RTU 3000 Family Multiple Vulnerabilities (ssa-756638)	Vulnerability - level 4	Vuln
591121	Siemens SIMATIC S7-1200 CPU Family Version 4 Vulnerability (ssa-507847,ICSA-18-282-04)	Vulnerability - level 3	Vuln
591122	Siemens SCALANCE X-200 Authentication Bypass Vulnerability (ICSA-13-274-01,ssa-176087)	Vulnerability - level 5	Vuln
591123	Schneider Electric Modicon TM5 modules Multiple Vulnerabilities (SEVD-2021-285-06)	Vulnerability - level 5	Vuln
591124	FATEK Automation FvDesigner Vulnerability (ICSA-22-237-01)	Vulnerability - level 4	Vuln
591125	Omron CX-Programmer Vulnerability (ICSA-22-242-09)	Vulnerability - level 4	Vuln
591126	Siemens Simatic Weak Key Protection Vulnerability (ICSA-22-286-04, SSA-568427, SSB-898115)	Vulnerability - level 4	Vuln
591127	Siemens SIMATIC S7-1200 and S7-1500 CPU Families Weak Key Protection Vulnerability (SSA-568427,icsa-22-286-04)	Vulnerability - level 4	Vuln
591128	Siemens SIMATIC STEP 7 TIA Portal Improper Access Control Vulnerability (SSA-350757)	Vulnerability - level 4	Vuln
591129	Keysight N6854A Geolocation server and N6841A RF Sensor software Multiple Vulnerabilities (ICSA-22-146-01)	Vulnerability - level 5	Vuln
591130	Emerson ControlWave Vulnerability (ICSA-22-221-02)	Potential Vulnerability - level 4	Practice
591131	Moxa AWK-3131A iw_webs DecryptScriptFile file name Command Injection Vulnerability (TALOS-2019-0929)	Vulnerability - level 4	Vuln
591133	Siemens JT2GO Multiple Vulnerabilities (ICSA-21-350-08)	Vulnerability - level 4	Vuln
591137	Advantech OPC Server Buffer Overflow Vulnerability (ICSA-11-279-01)	Vulnerability - level 4	Vuln
591138	Emerson Rosemount X-STREAM Multiple Vulnerabilities (icsa-21-138-01)	Vulnerability - level 5	Vuln
591139	Siemens Industrial Products LLDP (Update D) Multiple Vulnerabilities (icsa-21-194-07, SSA-941426)	Vulnerability - level 5	Vuln
591140	Emerson WirelessHART Gateway Multiple Vulnerabilities (ICSA-21-278-02)	Vulnerability - level 4	Vuln
591141	AVEVA System Platform Sensitive Information Disclosure Vulnerability (ICSA-22-067-02)	Vulnerability - level 3	Vuln
591142	Rockwell Automation ISaGRAF Multiple Vulnerabilities (SEP-SA-2022-0001)	Vulnerability - level 4	Vuln
591143	Fuji Electric V-Server Remote Code Execution (RCE) Vulnerability (ICSA-18-254-01)	Vulnerability - level 4	Vuln
591144	Siemens JT2go Datalogics File Parsing Vulnerability (SSA-829738,icsa-22-195-07)	Vulnerability - level 4	Vuln

591145	Mitsubishi Electric Factory Automation Engineering Products (Update I) Denial of Service (DoS) Vulnerability (ICSA-20-212-04)	Vulnerability - level 5	Vuln
591146	Fuji Electric D300win Multiple Vulnerabilities (ICSA-22-242-05)	Vulnerability - level 5	Vuln
591147	Softing Secure Integration Server Multiple Vulnerabilities (ICSA-22-228-04)	Vulnerability - level 5	Vuln
591148	Hitachi Energy RTU500 series BCI Vulnerability (ICSA-21-336-04,8DBD000063)	Potential Vulnerability - level 4	Practice
591149	Hitachi Energy RTU500 series Vulnerability (ICSA-22-242-04,8DBD000103)	Potential Vulnerability - level 4	Practice
591150	Hitachi ABB Power Grids TropOS Multiple Vulnerabilities (ICSA-21-236-01,9AKK107992A4463)	Vulnerability - level 3	Vuln
591151	Hitachi Energy AFS660/AFS665 Vulnerability (ICSA-22-270-01,8DBD000122)	Vulnerability - level 5	Vuln
591155	Schneider Electric SOMOVE,ATV320,ATV340,ATV6xx,ATV9xx Arbitrary Code Execution Vulnerability (ICSA-18-065-02)	Vulnerability - level 4	Vuln
591160	Siemens Simcenter Femap Vulnerability (SSA-474231,icsa-22-195-04)	Vulnerability - level 4	Vuln
591164	Siemens SIMATIC NET PC Software Unquoted Search Path Vulnerability (SSA-312271)	Vulnerability - level 3	Vuln
591165	LS ELECTRIC XG5000 Vulnerability (ICSA-22-228-02)	Vulnerability - level 2	Vuln
591166	Rockwell Automation ISaGRAF, CCW, SISW Vulnerability (ICSA-22-095-01, PN1589)	Vulnerability - level 4	Vuln
591170	Mitsubishi Electric GT SoftGOT2000 Multiple Vulnerabilities (ICSA-22-221-01)	Vulnerability - level 5	Vuln
591171	Siemens SICAM P850 and P855 Devices Multiple Vulnerabilities (SSA-572005,ICSA-22-286-09)	Vulnerability - level 4	Vuln
591174	Siemens SIMATIC PCS 7, Step 7, Starter Incorrect Permission Assignment Vulnerability (SSA-661034)	Vulnerability - level 4	Vuln
591179	Trihedral VTScada Denial of Service (DoS) Vulnerability (ICSA-22-300-04)	Vulnerability - level 4	Vuln
591180	Siemens JT2Go Multiple Vulnerabilities (ICSA-22-314-09, SSA-120378)	Vulnerability - level 4	Vuln
591181	Advantech R-SeeNet Multiple Vulnerabilities (ICSA-22-291-01) (CVE-2022-3387)	Vulnerability - level 3	Vuln
591182	Advantech R-SeeNet Multiple Vulnerabilities (ICSA-22-291-01) (CVE-2022-3386,CVE-2022-3385)	Vulnerability - level 5	Vuln
591183	Omron NJ/NX-series Machine Automation Controllers Vulnerability (ICSA-22-314-07)	Vulnerability - level 4	Vuln
591184	Mitsubishi Electric Multiple Factory Automation Products (Update C) Multiple Vulnerabilities (ICSA-22-221-01)	Vulnerability - level 5	Vuln
591185	Moxa MGate Protocol Gateways Vulnerability (ICSA-21-357-01)	Vulnerability - level 4	Vuln
591186	Mitsubishi Electric Air Conditioning Systems Multiple Vulnerabilities (ICSA-22-160-01)	Vulnerability - level 4	Vuln
591187	Siemens RUGGEDCOM ROS (Update A) Vulnerability (ICSA-22-195-18, SSA-840800)	Vulnerability - level 4	Vuln
591188	Siemens SCALANCE W1750D Multiple Vulnerabilities (ICSA-22-314-10, SSA-506569)	Vulnerability - level 5	Vuln
591189	Siemens RUGGEDCOM ROS (Update A) Vulnerability (ICSA-22-258-03, SSA-459643)	Vulnerability - level 4	Vuln
591192	Siemens Linux-based Products (Update J) Vulnerability (ICSA-21-131-03, SSA-324955)	Vulnerability - level 4	Vuln
591193	Mitsubishi Electric GT SoftGOT2000 OS COMMAND INJECTION Vulnerability (ICSA-22-319-01, 2022-012)	Vulnerability - level 5	Vuln
591194	Siemens TIA Portal Local Privilege Escalation Vulnerability (SSA-629512)	Vulnerability - level 4	Vuln
591196	Siemens SIMATIC S7-300 CPU Vulnerability (ICSA-19-043-04, SSA-306710)	Potential Vulnerability - level 4	Practice
591197	Siemens SIMATIC S7-300 Denial of Service (DoS) Vulnerability (ICSA-16-161-01, SSA-818183)	Vulnerability - level 4	Vuln

591198	Siemens Mendix XPath Constraint Vulnerability (SSA-148641)	Potential Vulnerability - level 4	Practice
591199	Siemens PROFINET Stack Integrated on Interniche Stack (Update D) Vulnerability (ICSA-22-104-06, SSA-446448)	Vulnerability - level 4	Vuln
591200	Siemens Mendix (Update B) Sensitive Information Disclosure Vulnerability (icsa-22-104-07, SSA-414513)	Vulnerability - level 4	Vuln
591201	Siemens WinCC (TIA Portal), IPC Diagbase and Simatic Step 7 (TIA Portal) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (SSA-179516)	Vulnerability - level 3	Vuln
591205	Siemens SCALANCE X-200 and X-200IRT Families Cross-Site Scripting (XSS) Vulnerability (ICSA-22-286-15, ssa-501891)	Vulnerability - level 3	Vuln
591207	Siemens SIMATIC Industrial Products Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-041-01, SSA-838121)	Vulnerability - level 4	Vuln
591210	Siemens SIMATIC S7-1500 CPU Improper Input Validation Multiple Vulnerabilities (ICSA-19-036-04, SSA-180635)	Vulnerability - level 4	Vuln
591211	Siemens LOGO! 8 BM Devices Multiple Vulnerabilities (ICSA-22-286-13, SSA-955858)	Potential Vulnerability - level 5	Practice
591212	Siemens SIMATIC Cross-Site Request Forgery (CSRF) Vulnerability (ICSA-22-314-02, SSA-478960)	Vulnerability - level 3	Vuln
591221	Siemens SINEC NMS and SINEMA Server Multiple Vulnerabilities (SSA-685781 V1.1)	Vulnerability - level 5	Vuln
591222	Siemens APOGEE, TALON and Desigo PXC/PXM Products Uncontrolled Resource Consumption Vulnerability (SSA-935500, ICSA-22-286-12)	Vulnerability - level 4	Vuln
591225	Mitsubishi Electric MELSEC iQ-R Series Improper Input Validation Vulnerability (icsa-22-335-01)	Vulnerability - level 4	Vuln
591227	Mitsubishi Electric FA Engineering Software GXWorks3 Multiple Vulnerabilities (ICSA-22-333-05)	Potential Vulnerability - level 5	Practice
591228	Siemens SIMATIC S7-PLCSIM Advanced Vulnerability (icsa-21-152-01, SSA-434534)	Vulnerability - level 5	Vuln
591229	Moxa Arm-based Computer Improper Privilege Management Vulnerability (ICSA-22-326-05, MPSA-221108)	Vulnerability - level 4	Vuln
591231	Siemens SINUMERIK ONE and SINUMERIK MC Insufficiently Protected Credentials Vulnerability (ICSA-22-314-04, ssa-568428)	Vulnerability - level 4	Vuln
591233	"B and R" Automation Studio Denial of Service (DoS) Vulnerability (ADVISORY_04-2022)	Potential Vulnerability - level 4	Practice
591234	GE Proficy CIMPLICITY Sensitive Information Disclosure Vulnerability (ICSA-22-053-02)	Vulnerability - level 5	Vuln
591235	ARC Informatique PcVue (Update A) Sensitive Information Disclosure Vulnerability (ICSA-22-235-01)	Vulnerability - level 3	Vuln
591237	ABB PCM600 Cleartext Credentials Sensitive Information Disclosure Vulnerability (ICSA-22-333-02, ABBVREP0086)	Vulnerability - level 3	Vuln
591243	Siemens SIMATIC S7-1200/1500 CPU family Resource Exhaustion Vulnerability (ICSA-18-317-05, SSA-584286)	Vulnerability - level 4	Vuln
591244	Siemens SICAM Q100 Session Fixation, Improper Input Validation Multiple Vulnerabilities (ICSA-22-314-11, SSA-570294)	Vulnerability - level 4	Vuln
591247	Mitsubishi Electric GOT2000 Series Improper Input Validation Vulnerability (ICSA-22-333-01, 2022-016)	Vulnerability - level 3	Vuln
591249	Emerson DeltaV Distributed Control System Multiple Vulnerabilities (ICSA-22-181-03)	Vulnerability - level 4	Vuln
591250	Rockwell Automation Logix controllers Improper Input Validation Vulnerability (ICSA-22-342-03)	Vulnerability - level 4	Vuln
591251	Omron NJ/NX-series Machine Automation Controllers Multiple Vulnerabilities (ICSA-22-314-08, OMSR-2022-001)	Vulnerability - level 4	Vuln
591253	Siemens SIMATIC Controllers and TIM Incorrect Authorization Vulnerability (ICSA-21-257-23, SSA-865327)	Vulnerability - level 3	Vuln
591254	Mitsubishi Electric MELSEC iQ-R, iQ-L Series and MELIPC Series Improper Resource Shutdown or Release Vulnerability (ICSA-22-356-03, 2022-018)	Vulnerability - level 4	Vuln

591255	Siemens SIMATIC Controllers and TIM Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-03, SSA-382653)	Vulnerability - level 4	Vuln
591256	Schneider Electric Tricon Communication Module Multiple Vulnerabilities (ICSA-20-205-01, SESB-2020-105-01)	Vulnerability - level 5	Vuln
591257	Siemens SCALANCE SC-600 Family Multiple Vulnerabilities (ICSA-22-349-18, SSA-333517)	Vulnerability - level 4	Vuln
591258	Siemens SIPROTEC 5 Devices Denial of Service (DoS) Vulnerability (ICSA-22-349-11, SSA-552874)	Vulnerability - level 4	Vuln
591259	Siemens RUGGEDCOM Devices Inadequate Encryption Strength Vulnerability (ICSA-22-069-01, SSA-764417)	Vulnerability - level 3	Vuln
591260	Siemens LOGO! Firmware Authenticity Vulnerability (ICSA-22-286-01, SSA-928782)	Vulnerability - level 3	Vuln
591261	Siemens MindConnect, S7-1200/1500 CPU family, ET 200SP Open Controller Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (ICSA-18-226-02, SSA-179516)	Vulnerability - level 3	Vuln
591263	Moxa EDR-G902 and EDR-G903 Series Routers Stack-based Buffer Overflow Vulnerability (ICSA-20-196-02, MPESA-200502)	Vulnerability - level 5	Vuln
591264	Omron CX-Programmer Out-of-bounds Write Vulnerability (ICSA-22-356-04)	Vulnerability - level 4	Vuln
591266	Siemens SCALANCE X-300/X408 Switch Family Denial of Service (DoS) Multiple Vulnerabilities (ICSA-15-020-01, SSA-321046)	Vulnerability - level 4	Vuln
591268	Mitsubishi Electric MELSEC iQ-R Series Denial of Service (DoS) Vulnerability (ICSA-20-317-01, 2020-015)	Vulnerability - level 4	Vuln
591269	Mitsubishi Electric MELSEC-F Series Denial of Service (DoS) Vulnerability (ICSA-22-013-01)	Vulnerability - level 4	Vuln
591270	Rockwell Automation MicroLogix 1100 and 1400 Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-354-04)	Potential Vulnerability - level 4	Practice
591272	Honeywell IQ Series Controllers Cleartext Transmission of Sensitive Information Vulnerability (ICSA-22-242-08)	Vulnerability - level 3	Vuln
591273	Siemens APOGEE and TALON Improper Access Control Vulnerability (ICSA-22-349-16, SSA-180579)	Vulnerability - level 3	Vuln
591274	Moxa UC Series Improper Physical Access Control Vulnerability (ICSA-22-333-04)	Vulnerability - level 4	Vuln
591278	AutomationDirect DirectLOGIC with Ethernet Communication Modules Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-167-03)	Potential Vulnerability - level 5	Practice
591279	Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS), Hijacking of web sessions Multiple Vulnerabilities (ICSA-22-349-02, SSA-363821)	Vulnerability - level 5	Vuln
591280	Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)	Vulnerability - level 5	Vuln
591281	Phoenix Contact FL NAT SMx Improper Access Control Vulnerability (ICSA-19-155-02, VDE-2019-006)	Vulnerability - level 4	Vuln
591284	General Electric Multilink Switch Rivest Shamir Adleman (RSA) Private Key and Denial of Service (DoS) Multiple Vulnerabilities (ICSA-15-013-04A)	Vulnerability - level 3	Vuln
591287	Siemens SICAM A8000 Web Server Module Improper Access Control Vulnerability (ICSA-22-223-05, SSA-185638)	Vulnerability - level 4	Vuln
591289	Automation Direct CLICK PLC CPU Modules Unprotected Storage of Credentials Multiple Vulnerabilities (ICSA-21-166-02)	Vulnerability - level 5	Vuln
591290	Schneider Electric Saitel DR RTU Denial of Service (DoS) Vulnerability (SEVD-2022-347-02)	Vulnerability - level 5	Vuln
591291	Siemens SCALANCE and RUGGEDCOM Products Denial of Service (DoS) Vulnerability (ICSA-22-286-08, SSA-697140)	Vulnerability - level 4	Vuln
591292	Siemens APOGEE/TALON Field Panels Predictable Exact Value from Previous Values Vulnerability (ICSA-22-349-10, SSA-436469)	Vulnerability - level 3	Vuln
591294	Rockwell Automation ThinManager ThinServer Heap-based Buffer Overflow Vulnerability (ICSA-22-270-03)	Vulnerability - level 5	Vuln

591298	Phoenix Contact mGuard Denial of Service (DoS) Vulnerability (VDE-2017-001)	Vulnerability - level 4	Vuln
591300	Red Lion Crimson Path Traversal Vulnerabilities(ICSA-22-321-01)	Vulnerability - level 3	Vuln
591305	Siemens JT2Go Multiple Vulnerabilities (SSA-360681)	Vulnerability - level 4	Vuln
591307	Siemens S7-1500 CPU devices Missing Immutable Root of Trust in Hardware Vulnerability (ICSA-23-012-08, SSA-482757)	Vulnerability - level 3	Vuln
591308	ABB AFS66x WindRiver VxWorks IPNet Multiple Vulnerabilities (ABBVU-PGGA-AFS66X-0252019)	Vulnerability - level 5	Vuln
591311	Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)	Vulnerability - level 5	Vuln
591314	Siemens Automation License Manager Multiple Vulnerabilities (ICSA-23-012-10,SSA-476715)	Vulnerability - level 5	Vuln
591317	Siemens EN100 Ethernet Module Memory Buffer Vulnerability (SSA-865333)	Potential Vulnerability - level 4	Practice
591318	Delta Industrial Automation 4G Router DX-3021 Command Injection Vulnerability (ICSA-22-354-05)	Vulnerability - level 5	Vuln
591319	Honeywell Experion LX Missing Authentication for Critical Function Vulnerability (ICSA-22-242-07)	Vulnerability - level 5	Vuln
591321	General Electric MultiLink Managed Switches Hard-coded Credentials Vulnerability (GET-20042)	Vulnerability - level 5	Vuln
591328	Siemens Mendix Improper Access Control Vulnerability (SSA-433782)	Vulnerability - level 4	Vuln
591329	Siemens SIMATIC S7-1200 CPU Family Web Vulnerability (SSA-597212)	Vulnerability - level 3	Vuln
591330	Siemens EN100 Ethernet Communication Module Denial-of-Service Vulnerabilities (SSA-325546)	Potential Vulnerability - level 4	Practice
591334	Siemens SCALANCE Denial of Service (DoS) Multiple Vulnerabilities (SSA-710008, ICSA-22-223-07)	Vulnerability - level 4	Vuln
591337	Siemens JT2Go Multiple Vulnerabilities (ICSA-22-349-20,SSA-700053)	Vulnerability - level 4	Vuln
591338	Siemens SCALANCE and RUGGEDCOM Products Privilege Escalation Vulnerability (ICSA-22-286-11, SSA-552702)	Vulnerability - level 4	Vuln
591341	Moxa AWK-3131A Series Multiple Vulnerabilities (MPSA-200203)	Vulnerability - level 5	Vuln
591343	Horner Automation Remote Compact Controller Inadequate Encryption Strength, Use of Hard-coded Cryptographic Key, Excessive Reliance on Global Variables Multiple Vulnerabilities (ICSA-22-335-02)	Vulnerability - level 5	Vuln
591344	Siemens SCALANCE W1750D Cryptographic issues Vulnerability (SSA-464260, ICSA-18-282-02)	Vulnerability - level 3	Vuln
591347	Black Box KVM Path Traversal Vulnerability (ICSA-23-010-01)	Vulnerability - level 4	Vuln
591350	General Electric D20MX Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (PRSN-0006)	Vulnerability - level 4	Vuln
591351	Eaton Lighting Systems EG2 Web Control Authentication Bypass Multiple Vulnerabilities (ICSA-16-061-03, ETN-VA-2016-1000)	Vulnerability - level 4	Vuln
591360	ABB AC 800M WindRiver VxWorks IPNet Multiple Vulnerabilities (ABBVU-800xAICON-OL-5114-001)	Potential Vulnerability - level 5	Practice
591362	Eaton xComfort ECI authentication bypass Vulnerability (ETN-VA-2017-1001)	Vulnerability - level 4	Vuln
591363	Ovarro TBox MS-CPU32, TBox MS-CPU32-S2, TBox LT2, TBox TG2, TBox RM2 product families Vulnerability (TBOX-SA-2021-0005)	Vulnerability - level 4	Vuln
591364	Ovarro LT2 / RM2 / TG2 / CPU32 / CPU32-S2 Product Families Malicious Code Execution Vulnerability (TBOX-SA-2021-0006)	Vulnerability - level 5	Vuln
591365	Ovarro LT2 / RM2 / TG2 / CPU32 / CPU32-S2 Product Families Shell Commands Execution Vulnerability (TBOX-SA-2021-0008)	Vulnerability - level 5	Vuln
591366	Hitachi Energy AFF660/665 Series Stack-based Buffer Overflow Vulnerability (ICSA-22-263-02, 8DBD000122)	Potential Vulnerability - level 5	Practice
591369	ABB CI845 WindRiver VxWorks IPNet Multiple Vulnerabilities (ABBVU-IACT-800xAIOE-OL-1000-10017)	Vulnerability - level 5	Vuln

591370	Siemens SIMATIC HMI Panels Improper Input Validation Vulnerability (ICSA-22-286-14, SSA-384224)	Vulnerability - level 4	Vuln
591371	Siemens SCALANCE X200 IRT Improper Input Validation Vulnerability (ICSA-23-047-02, SSA-617755)	Vulnerability - level 4	Vuln
591372	Rockwell Automation GuardLogix and ControlLogix controllers Improper Input Validation Vulnerability (icsa-22-354-02)	Vulnerability - level 4	Vuln
591376	Siemens Climatix POL909 Cross-Site Scripting (XSS), Improper Access Control Multiple Vulnerabilities (SSA-252466, ICSA-22-069-07)	Vulnerability - level 3	Vuln
591377	ABB Relion 670 series Version 2.0 Transmission Control Protocol (TCP) Predictability Multiple Vulnerabilities (1MRG023264)	Vulnerability - level 3	Vuln
591379	LS ELECTRIC XG5000 Inadequate Encryption Strength Vulnerability (ICSA-22-228-02)	Vulnerability - level 3	Vuln
591380	Fuji Electric Tellus Lite V-Simulator Multiple Vulnerabilities (ICSA-22-354-01)	Vulnerability - level 4	Vuln
591383	ABB RTU500 series "Transmission Control Protocol (TCP) Predictability Multiple Vulnerabilities (ABB-VU-PGGA-1KGT090284)	Vulnerability - level 3	Vuln
591384	ABB Relion 670 series "Transmission Control Protocol (TCP) Predictability Multiple Vulnerabilities (1MRG028797)	Vulnerability - level 3	Vuln
591385	Mitsubishi Electric MELSEC C Controller Module and MELIPC Series MI5000 Transmission Control Protocol/Internet Protocol (TCP/IP) function Multiple Vulnerabilities (2019-003)	Potential Vulnerability - level 5	Practice
591386	Moxa PT-7528 and PT-7828 Series Ethernet Switches Use of Hard-coded Credentials Multiple Vulnerabilities (ICSA-20-056-03, MP5A-190904)	Vulnerability - level 5	Vuln
591387	Landis+Gyr E850 Reliance on Cookies without Validation and Integrity Vulnerability (ICSA-23-026-07)	Vulnerability - level 3	Vuln
591392	Delta Electronics CNCSoft ScreenEditor Stack-based Buffer Overflow Vulnerability (ICSA-23-026-01)	Vulnerability - level 4	Vuln
591394	ABB TropOS wireless mesh products WPA2 Key Reinstallation Multiple Vulnerabilities (ICSA-17-318-02A, ABBVU-PGGA-1KHW028907)	Vulnerability - level 4	Vuln
591395	General Electric Universal Relay (UR) family of products Distributed Network Protocol (DNP3) Implementation Vulnerability (GET-20046A)	Vulnerability - level 4	Vuln
591397	Siemens Scalance W-7xx (a/b/g) Product Family Improper Authentication Multiple Vulnerabilities (SSA-120908, icsa-13-213-01)	Vulnerability - level 5	Vuln
591398	Siemens CPC80 Firmware of SICAM A8000 Devices Denial of Service (DoS) Vulnerability (SSA-491621, ICSA-22-195-14)	Vulnerability - level 4	Vuln
591399	General Electric D20MX Transmission Control Protocol (TCP) Initial Sequence Number Vulnerability (PRBT-0375)	Vulnerability - level 3	Vuln
591400	Siemens SICAM MMU, SICAM T and SICAM SGU Multiple Vulnerabilities (SSA-305120, ICSA-20-196-03)	Vulnerability - level 5	Vuln
591401	Siemens Ruggedcom ROS, SCALANCE Improper Access Control Multiple Vulnerabilities (ICSA-17-271-01B, SSA-856721)	Vulnerability - level 4	Vuln
591406	Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)	Vulnerability - level 5	Vuln
591411	Schneider Electric APC Easy UPS Online Monitoring Software Multiple Vulnerabilities (SEVD-2022-347-01 V2.0)	Vulnerability - level 5	Vuln
591416	Delta Electronics DMARS Sensitive Information Disclosure Vulnerability (ICSA-22-104-01)	Vulnerability - level 3	Vuln
591422	Delta Electronics InfraSuite Device Master Multiple Security Vulnerabilities (ICSA-23-080-02)	Vulnerability - level 5	Vuln
591423	Siemens Desigo Control Point Devices (PXM and PXG3) Webserver Multiple Security Vulnerabilities (SSA-360783)	Vulnerability - level 4	Vuln
610098	Google Pixel Android November 2017 Security Patch Missing	Vulnerability - level 5	Vuln
610109	Google Pixel Android June 2018 Security Patch Missing	Vulnerability - level 5	Vuln

610116	Google Android Devices May 2016 Security Patch Missing	Potential Vulnerability - level 4	Practice
610118	Google Android Devices July 2016 Security Patch Missing	Potential Vulnerability - level 4	Practice
610119	Google Android Devices August 2016 Security Patch Missing	Potential Vulnerability - level 4	Practice
610123	Google Android Devices December 2016 Security Patch Missing	Potential Vulnerability - level 4	Practice
610124	Google Android Devices January 2017 Security Patch Missing	Potential Vulnerability - level 4	Practice
610126	Google Android Devices March 2017 Security Patch Missing	Potential Vulnerability - level 4	Practice
610128	Google Android Devices May 2017 Security Patch Missing	Potential Vulnerability - level 4	Practice
610130	Google Android Devices July 2017 Security Patch Missing	Potential Vulnerability - level 4	Practice
610134	Google Android Devices November 2017 Security Patch Missing	Potential Vulnerability - level 4	Practice
610141	Google Android Devices July 2018 Security Patch Missing	Potential Vulnerability - level 4	Practice
610149	Apple iOS 9.3.2 Security Update Missing	Vulnerability - level 5	Vuln
610156	Apple iOS 10.3.3 Security Update Missing	Vulnerability - level 5	Vuln
610157	Apple iOS 11.1 Security Update Missing	Vulnerability - level 5	Vuln
610158	Apple iOS 11.2 Security Update Missing	Vulnerability - level 5	Vuln
610173	Google Android May 2016 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610175	Google Android July 2016 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610176	Google Android August 2016 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610180	Google Android December 2016 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610181	Google Android January 2017 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610183	Google Android March 2017 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610185	Google Android May 2017 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610187	Google Android July 2017 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610191	Google Android November 2017 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610199	Google Android July 2018 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610205	Google Android May 2016 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610207	Google Android July 2016 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610208	Google Android August 2016 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610212	Google Android December 2016 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610214	Google Android February 2017 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610215	Google Android March 2017 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610218	Google Android June 2017 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610219	Google Android July 2017 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610223	Google Android November 2017 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610231	Google Android July 2018 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610234	Google Android October 2018 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610247	Google Android June 2018 Security Patch Missing for Huawei EMUI	Vulnerability - level 5	Vuln
610250	Google Android September 2018 Security Patch Missing for Huawei EMUI	Vulnerability - level 5	Vuln
610331	Google Android Devices April 2021 Security Patch Missing	Potential Vulnerability - level 4	Practice
610340	Google Android May 2021 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610341	Google Android May 2021 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610342	Apple iOS 14.6 and iPadOS 14.6 Security Update Missing (HT212528)	Vulnerability - level 5	Vuln
610343	Google Pixel Android June 2021 Security Patch Missing	Vulnerability - level 5	Vuln

610347	Google Android May 2021 Security Patch Missing for Huawei EMUI	Vulnerability - level 5	Vuln
610349	Apple iOS 14.7 and iPadOS 14.7 Security Update Missing	Vulnerability - level 5	Vuln
610360	Google Android August 2021 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610373	Google Android Devices October 2021 Security Patch Missing	Potential Vulnerability - level 4	Practice
610381	Google Android November 2021 Security Patch Missing for Huawei EMUI	Vulnerability - level 5	Vuln
610382	Google Android November 2021 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610383	Google Android November 2021 Security Patch Missing for LGE	Vulnerability - level 5	Vuln
610390	Google Android Devices January 2022 Security Patch Missing	Potential Vulnerability - level 4	Practice
610394	Apple iOS 15.2.1 and iPadOS 15.2.1 Security Update Missing	Vulnerability - level 5	Vuln
610398	Google Android February 2022 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610416	Apple iOS 15.5 and iPadOS 15.5 Security Update Missing (HT213258)	Vulnerability - level 5	Vuln
610429	Google Android Devices September 2022 Security Patch Missing	Potential Vulnerability - level 4	Practice
610430	Google Android September 2022 Security Patch Missing for Huawei EMUI	Vulnerability - level 5	Vuln
610431	Google Android September 2022 Security Patch Missing for Samsung	Vulnerability - level 5	Vuln
610432	Google Pixel Android August 2022 Security Patch Missing	Vulnerability - level 5	Vuln
610439	Google Android October 2022 Security Patch Missing for Huawei EMUI	Vulnerability - level 5	Vuln
610451	Google Pixel Android December 2022 Security Patch Missing	Vulnerability - level 5	Vuln
610464	Google Android January 2023 Security Patch Missing for Huawei EMUI	Vulnerability - level 5	Vuln
62074	Squid Proxy Same Origin Bypass Local Security Vulnerability (SQUID-2011:1)	Potential Vulnerability - level 3	Practice
630033	Philips HealthSuite For Android Weak Encryption Local Security Weakness Vulnerability	Vulnerability - level 2	Vuln
630035	Marine Pro Observer For Android Information Disclosure Vulnerability	Vulnerability - level 3	Vuln
630126	ShoreTel Mobility Client For iOS MiTM Vulnerability	Vulnerability - level 1	Vuln
630235	Grandstream Wave For Android Improper Access Contro Vulnerability	Vulnerability - level 2	Vuln
630522	Siemens SIMATIC WinCC Sm@rtClient Application Privilage Escalation Vulnerability	Vulnerability - level 3	Vuln
630523	Siemens SPCanywhere App For Android Multiple Vulnerabilities	Vulnerability - level 3	Vuln
630524	Siemens Sm@rtClient For Android Password Storage Vulnerability	Vulnerability - level 2	Vuln
630525	Siemens SIMATIC WinCC Sm@rtClient for Android Authentication Bypass Vulnerability	Vulnerability - level 4	Vuln
630526	SIMATIC WinCC OA UI Improper Privilege Management Vulnerability	Vulnerability - level 3	Vuln
630527	SIMATIC WinCC OA Operator For iOS Missing Encryption of Sensitive Data Vulnerability	Vulnerability - level 3	Vuln
630528	Siemens Siveillance VMS Deserialization of Untrusted Data Vulnerability	Vulnerability - level 4	Vuln
630529	Siemens Siveillance VMS Video Improper Certificate Validation Vulnerability	Vulnerability - level 3	Vuln
670173	EulerOS Security Update for dnsmasq (EulerOS-SA-2021-1673)	Vulnerability - level 4	Vuln
670184	EulerOS Security Update for iscsi-initiator-utils (EulerOS-SA-2021-1683)	Vulnerability - level 3	Vuln
670185	EulerOS Security Update for kernel (EulerOS-SA-2021-1684)	Vulnerability - level 4	Vuln
670194	EulerOS Security Update for openldap (EulerOS-SA-2021-1693)	Vulnerability - level 3	Vuln

670196	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1695)	Vulnerability - level 2	Vuln
670197	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL111d) (EulerOS-SA-2021-1696)	Vulnerability - level 2	Vuln
670245	EulerOS Security Update for pki-core (EulerOS-SA-2021-1831)	Vulnerability - level 3	Vuln
670250	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL098e) (EulerOS-SA-2021-1826)	Vulnerability - level 3	Vuln
670251	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1825)	Vulnerability - level 3	Vuln
670252	EulerOS Security Update for openldap (EulerOS-SA-2021-1824)	Vulnerability - level 3	Vuln
670282	EulerOS Security Update for grub2 (EulerOS-SA-2021-1794)	Vulnerability - level 4	Vuln
670315	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL11d) (EulerOS-SA-2021-1909)	Vulnerability - level 3	Vuln
670316	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL098e) (EulerOS-SA-2021-1908)	Vulnerability - level 3	Vuln
670317	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1907)	Vulnerability - level 3	Vuln
670318	EulerOS Security Update for openldap (EulerOS-SA-2021-1906)	Vulnerability - level 3	Vuln
670324	EulerOS Security Update for grub2 (EulerOS-SA-2021-1900)	Vulnerability - level 4	Vuln
670330	EulerOS Security Update for bind (EulerOS-SA-2021-1894)	Vulnerability - level 3	Vuln
670342	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1882)	Vulnerability - level 3	Vuln
670343	EulerOS Security Update for openldap (EulerOS-SA-2021-1881)	Vulnerability - level 3	Vuln
670349	EulerOS Security Update for grub2 (EulerOS-SA-2021-1875)	Vulnerability - level 4	Vuln
670356	EulerOS Security Update for curl (EulerOS-SA-2021-1868)	Vulnerability - level 2	Vuln
670359	EulerOS Security Update for bind (EulerOS-SA-2021-1865)	Vulnerability - level 3	Vuln
670364	EulerOS Security Update for bind (EulerOS-SA-2021-1766)	Vulnerability - level 3	Vuln
670369	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1956)	Vulnerability - level 3	Vuln
670372	EulerOS Security Update for open-iscsi (EulerOS-SA-2021-1953)	Vulnerability - level 4	Vuln
670376	EulerOS Security Update for grub2 (EulerOS-SA-2021-1948)	Vulnerability - level 4	Vuln
670383	EulerOS Security Update for curl (EulerOS-SA-2021-1942)	Vulnerability - level 2	Vuln
670386	EulerOS Security Update for bind (EulerOS-SA-2021-1939)	Vulnerability - level 3	Vuln
670390	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1935)	Vulnerability - level 3	Vuln
670393	EulerOS Security Update for open-iscsi (EulerOS-SA-2021-1932)	Vulnerability - level 4	Vuln
670398	EulerOS Security Update for grub2 (EulerOS-SA-2021-1927)	Vulnerability - level 4	Vuln
670404	EulerOS Security Update for curl (EulerOS-SA-2021-1921)	Vulnerability - level 2	Vuln
670414	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-1985)	Vulnerability - level 2	Vuln
670424	EulerOS Security Update for bind (EulerOS-SA-2021-1975)	Vulnerability - level 3	Vuln
670431	EulerOS Security Update for bind (EulerOS-SA-2021-1918)	Vulnerability - level 3	Vuln
670437	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-2063)	Vulnerability - level 2	Vuln
670448	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-2052)	Vulnerability - level 2	Vuln
670460	EulerOS Security Update for grub2 (EulerOS-SA-2021-2218)	Vulnerability - level 3	Vuln
670470	EulerOS Security Update for openssl1.1.1d (EulerOS-SA-2021-2225)	Vulnerability - level 2	Vuln
670478	EulerOS Security Update for bind (EulerOS-SA-2021-2236)	Vulnerability - level 3	Vuln
670491	EulerOS Security Update for libxml2 (EulerOS-SA-2021-2249)	Vulnerability - level 4	Vuln
670493	EulerOS Security Update for openldap (EulerOS-SA-2021-2251)	Vulnerability - level 3	Vuln
670504	EulerOS Security Update for bind (EulerOS-SA-2021-2262)	Vulnerability - level 3	Vuln
670517	EulerOS Security Update for libxml2 (EulerOS-SA-2021-2275)	Vulnerability - level 4	Vuln
670519	EulerOS Security Update for openldap (EulerOS-SA-2021-2277)	Vulnerability - level 3	Vuln
670548	EulerOS Security Update for libxml2 (EulerOS-SA-2021-2306)	Vulnerability - level 4	Vuln
670552	EulerOS Security Update for openldap (EulerOS-SA-2021-2310)	Vulnerability - level 3	Vuln
670554	EulerOS Security Update for postgresql (EulerOS-SA-2021-2312)	Vulnerability - level 3	Vuln
670562	EulerOS Security Update for bind (EulerOS-SA-2021-2320)	Vulnerability - level 3	Vuln

670581	EulerOS Security Update for libxml2 (EulerOS-SA-2021-2339)	Vulnerability - level 4	Vuln
670584	EulerOS Security Update for openldap (EulerOS-SA-2021-2342)	Vulnerability - level 3	Vuln
670586	EulerOS Security Update for postgresql (EulerOS-SA-2021-2344)	Vulnerability - level 3	Vuln
670596	EulerOS Security Update for bind (EulerOS-SA-2021-2354)	Vulnerability - level 3	Vuln
670618	EulerOS Security Update for grub2 (EulerOS-SA-2021-2376)	Vulnerability - level 4	Vuln
670623	EulerOS Security Update for httpd (EulerOS-SA-2021-2381)	Vulnerability - level 4	Vuln
670648	EulerOS Security Update for libxml2 (EulerOS-SA-2021-2406)	Vulnerability - level 4	Vuln
670655	EulerOS Security Update for nss (EulerOS-SA-2021-2413)	Vulnerability - level 2	Vuln
670657	EulerOS Security Update for openldap (EulerOS-SA-2021-2415)	Vulnerability - level 3	Vuln
670658	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-2416)	Vulnerability - level 3	Vuln
670659	EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) openssl098e (EulerOS-SA-2021-2417)	Vulnerability - level 3	Vuln
670660	EulerOS Security Update for Open Secure Sockets Layer110f (openssl110f) (EulerOS-SA-2021-2418)	Vulnerability - level 3	Vuln
670667	EulerOS Security Update for postgresql (EulerOS-SA-2021-2426)	Vulnerability - level 3	Vuln
670698	EulerOS Security Update for Compat-Open Secure Sockets Layer10 (compat-openssl10) (EulerOS-SA-2021-2456)	Vulnerability - level 3	Vuln
670705	EulerOS Security Update for httpd (EulerOS-SA-2021-2463)	Vulnerability - level 4	Vuln
670742	EulerOS Security Update for httpd (EulerOS-SA-2021-2500)	Vulnerability - level 4	Vuln
670771	EulerOS Security Update for httpd (EulerOS-SA-2021-2529)	Vulnerability - level 4	Vuln
670784	EulerOS Security Update for shim (EulerOS-SA-2021-2542)	Vulnerability - level 3	Vuln
670795	EulerOS Security Update for httpd (EulerOS-SA-2021-2553)	Vulnerability - level 4	Vuln
670808	EulerOS Security Update for shim (EulerOS-SA-2021-2566)	Vulnerability - level 3	Vuln
670831	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-2717)	Vulnerability - level 4	Vuln
670959	EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2021-2667)	Vulnerability - level 4	Vuln
670970	EulerOS Security Update for postgresql (EulerOS-SA-2021-2607)	Vulnerability - level 4	Vuln
670972	EulerOS Security Update for Compat-Open Secure Sockets Layer (compat-OpenSSL) (EulerOS-SA-2021-2625)	Vulnerability - level 4	Vuln
670993	EulerOS Security Update for Open Secure Sockets Layer111d (OpenSSL111d) (EulerOS-SA-2021-2668)	Vulnerability - level 4	Vuln
670996	EulerOS Security Update for libxml2 (EulerOS-SA-2021-2595)	Vulnerability - level 3	Vuln
671015	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-2692)	Vulnerability - level 4	Vuln
671019	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-2639)	Vulnerability - level 4	Vuln
671023	EulerOS Security Update for httpd (EulerOS-SA-2021-2586)	Vulnerability - level 5	Vuln
671031	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2021-2666)	Vulnerability - level 4	Vuln
671051	EulerOS Security Update for kernel (EulerOS-SA-2021-2663)	Vulnerability - level 3	Vuln
671073	EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2019-2643)	Vulnerability - level 2	Vuln
671109	EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2019-2509)	Vulnerability - level 3	Vuln
671133	EulerOS Security Update for bind (EulerOS-SA-2021-2572)	Vulnerability - level 4	Vuln
671140	EulerOS Security Update for openldap (EulerOS-SA-2021-2602)	Vulnerability - level 4	Vuln
671156	EulerOS Security Update for postgresql (EulerOS-SA-2021-2811)	Vulnerability - level 3	Vuln
671157	EulerOS Security Update for httpd (EulerOS-SA-2021-2803)	Vulnerability - level 5	Vuln
671161	EulerOS Security Update for golang (EulerOS-SA-2021-2802)	Vulnerability - level 3	Vuln
671166	EulerOS Security Update for httpd (EulerOS-SA-2021-2915)	Vulnerability - level 5	Vuln
671168	EulerOS Security Update for httpd (EulerOS-SA-2021-2923)	Vulnerability - level 5	Vuln
671176	EulerOS Security Update for shim (EulerOS-SA-2021-2927)	Vulnerability - level 4	Vuln
671177	EulerOS Security Update for shim (EulerOS-SA-2021-2920)	Vulnerability - level 4	Vuln
671187	EulerOS Security Update for golang (EulerOS-SA-2021-2930)	Vulnerability - level 5	Vuln
671190	EulerOS Security Update for httpd (EulerOS-SA-2021-2931)	Vulnerability - level 5	Vuln
671192	EulerOS Security Update for bind (EulerOS-SA-2022-1001)	Vulnerability - level 3	Vuln
671199	EulerOS Security Update for grub2 (EulerOS-SA-2022-1008)	Vulnerability - level 3	Vuln

671200	EulerOS Security Update for grub2 (EulerOS-SA-2022-1028)	Vulnerability - level 3	Vuln
671208	EulerOS Security Update for bind (EulerOS-SA-2022-1021)	Vulnerability - level 3	Vuln
671209	EulerOS Security Update for golang (EulerOS-SA-2022-1027)	Vulnerability - level 5	Vuln
671229	EulerOS Security Update for golang (EulerOS-SA-2022-1007)	Vulnerability - level 5	Vuln
671245	EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2022-1180)	Vulnerability - level 4	Vuln
671248	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1181)	Vulnerability - level 4	Vuln
671256	EulerOS Security Update for grub2 (EulerOS-SA-2022-1194)	Vulnerability - level 3	Vuln
671266	EulerOS Security Update for httpd (EulerOS-SA-2022-1167)	Vulnerability - level 5	Vuln
671286	EulerOS Security Update for golang (EulerOS-SA-2022-1254)	Vulnerability - level 5	Vuln
671293	EulerOS Security Update for httpd (EulerOS-SA-2022-1206)	Vulnerability - level 5	Vuln
671307	EulerOS Security Update for bind (EulerOS-SA-2022-1237)	Vulnerability - level 3	Vuln
671311	EulerOS Security Update for golang (EulerOS-SA-2022-1242)	Vulnerability - level 5	Vuln
671313	EulerOS Security Update for docker-engine (EulerOS-SA-2022-1239)	Vulnerability - level 4	Vuln
671321	EulerOS Security Update for docker-engine (EulerOS-SA-2022-1251)	Vulnerability - level 4	Vuln
671324	EulerOS Security Update for bind (EulerOS-SA-2022-1249)	Vulnerability - level 3	Vuln
671333	EulerOS Security Update for httpd (EulerOS-SA-2022-1225)	Vulnerability - level 5	Vuln
671343	EulerOS Security Update for curl (EulerOS-SA-2022-1265)	Vulnerability - level 2	Vuln
671356	EulerOS Security Update for bind (EulerOS-SA-2022-1261)	Vulnerability - level 3	Vuln
671359	EulerOS Security Update for golang (EulerOS-SA-2022-1269)	Vulnerability - level 4	Vuln
671364	EulerOS Security Update for busybox (EulerOS-SA-2022-1303)	Vulnerability - level 4	Vuln
671374	EulerOS Security Update for golang (EulerOS-SA-2022-1305)	Vulnerability - level 4	Vuln
671377	EulerOS Security Update for busybox (EulerOS-SA-2022-1287)	Vulnerability - level 4	Vuln
671378	EulerOS Security Update for golang (EulerOS-SA-2022-1289)	Vulnerability - level 4	Vuln
671381	EulerOS Security Update for uboot-tools (EulerOS-SA-2022-1312)	Vulnerability - level 5	Vuln
671382	EulerOS Security Update for uboot-tools (EulerOS-SA-2022-1296)	Vulnerability - level 5	Vuln
671412	EulerOS Security Update for libvncserver (EulerOS-SA-2022-1329)	Vulnerability - level 4	Vuln
671427	EulerOS Security Update for golang (EulerOS-SA-2022-1345)	Vulnerability - level 4	Vuln
671428	EulerOS Security Update for expat (EulerOS-SA-2022-1342)	Vulnerability - level 5	Vuln
671441	EulerOS Security Update for kernel (EulerOS-SA-2022-1366)	Vulnerability - level 4	Vuln
671446	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1455)	Vulnerability - level 3	Vuln
671447	EulerOS Security Update for expat (EulerOS-SA-2022-1425)	Vulnerability - level 5	Vuln
671452	EulerOS Security Update for golang (EulerOS-SA-2022-1449)	Vulnerability - level 4	Vuln
671457	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1434)	Vulnerability - level 3	Vuln
671459	EulerOS Security Update for expat (EulerOS-SA-2022-1446)	Vulnerability - level 5	Vuln
671472	EulerOS Security Update for golang (EulerOS-SA-2022-1428)	Vulnerability - level 4	Vuln
671487	EulerOS Security Update for busybox (EulerOS-SA-2022-1472)	Vulnerability - level 5	Vuln
671491	EulerOS Security Update for golang (EulerOS-SA-2022-1506)	Vulnerability - level 4	Vuln
671508	EulerOS Security Update for expat (EulerOS-SA-2022-1502)	Vulnerability - level 5	Vuln
671510	EulerOS Security Update for golang (EulerOS-SA-2022-1464)	Vulnerability - level 4	Vuln
671512	EulerOS Security Update for expat (EulerOS-SA-2022-1483)	Vulnerability - level 5	Vuln
671518	EulerOS Security Update for busybox (EulerOS-SA-2022-1463)	Vulnerability - level 5	Vuln
671524	EulerOS Security Update for golang (EulerOS-SA-2022-1473)	Vulnerability - level 4	Vuln
671527	EulerOS Security Update for golang (EulerOS-SA-2022-1487)	Vulnerability - level 4	Vuln
671562	EulerOS Security Update for libxml2 (EulerOS-SA-2022-1574)	Vulnerability - level 4	Vuln
671565	EulerOS Security Update for expat (EulerOS-SA-2022-1529)	Vulnerability - level 5	Vuln
671578	EulerOS Security Update for httpd (EulerOS-SA-2022-1569)	Vulnerability - level 5	Vuln
671588	EulerOS Security Update for expat (EulerOS-SA-2022-1562)	Vulnerability - level 5	Vuln
671595	EulerOS Security Update for subversion (EulerOS-SA-2022-1588)	Vulnerability - level 3	Vuln
671602	EulerOS Security Update for libxml2 (EulerOS-SA-2022-1541)	Vulnerability - level 4	Vuln
671610	EulerOS Security Update for golang (EulerOS-SA-2022-1534)	Vulnerability - level 5	Vuln
671616	EulerOS Security Update for golang (EulerOS-SA-2022-1566)	Vulnerability - level 5	Vuln
671618	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1649)	Vulnerability - level 3	Vuln

671620	EulerOS Security Update for expat (EulerOS-SA-2022-1659)	Vulnerability - level 5	Vuln
671621	EulerOS Security Update for golang (EulerOS-SA-2022-1660)	Vulnerability - level 4	Vuln
671628	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1663)	Vulnerability - level 3	Vuln
671642	EulerOS Security Update for expat (EulerOS-SA-2022-1645)	Vulnerability - level 5	Vuln
671645	EulerOS Security Update for golang (EulerOS-SA-2022-1646)	Vulnerability - level 4	Vuln
671657	EulerOS Security Update for xulrunner (EulerOS-SA-2022-1774)	Vulnerability - level 5	Vuln
671659	EulerOS Security Update for httpd (EulerOS-SA-2022-1730)	Vulnerability - level 5	Vuln
671663	EulerOS Security Update for bind (EulerOS-SA-2022-1705)	Vulnerability - level 3	Vuln
671675	EulerOS Security Update for libxml2 (EulerOS-SA-2022-1741)	Vulnerability - level 4	Vuln
671677	EulerOS Security Update for libvncserver (EulerOS-SA-2022-1740)	Vulnerability - level 4	Vuln
671703	EulerOS Security Update for kernel (EulerOS-SA-2022-1735)	Vulnerability - level 4	Vuln
671715	EulerOS Security Update for expat (EulerOS-SA-2022-1716)	Vulnerability - level 5	Vuln
671718	EulerOS Security Update for curl (EulerOS-SA-2022-1711)	Vulnerability - level 3	Vuln
671734	EulerOS Security Update for kernel (EulerOS-SA-2022-1791)	Vulnerability - level 4	Vuln
671737	EulerOS Security Update for bind (EulerOS-SA-2022-1783)	Vulnerability - level 4	Vuln
671739	EulerOS Security Update for httpd (EulerOS-SA-2022-1790)	Vulnerability - level 5	Vuln
671744	EulerOS Security Update for libxml2 (EulerOS-SA-2022-1810)	Vulnerability - level 4	Vuln
671745	EulerOS Security Update for bind (EulerOS-SA-2022-1800)	Vulnerability - level 4	Vuln
671749	EulerOS Security Update for kernel (EulerOS-SA-2022-1808)	Vulnerability - level 4	Vuln
671750	EulerOS Security Update for libxml2 (EulerOS-SA-2022-1793)	Vulnerability - level 4	Vuln
671754	EulerOS Security Update for golang (EulerOS-SA-2022-1805)	Vulnerability - level 5	Vuln
671755	EulerOS Security Update for golang (EulerOS-SA-2022-1788)	Vulnerability - level 5	Vuln
671757	EulerOS Security Update for expat (EulerOS-SA-2022-1786)	Vulnerability - level 5	Vuln
671758	EulerOS Security Update for httpd (EulerOS-SA-2022-1807)	Vulnerability - level 5	Vuln
671760	EulerOS Security Update for expat (EulerOS-SA-2022-1803)	Vulnerability - level 5	Vuln
671783	EulerOS Security Update for golang (EulerOS-SA-2022-1841)	Vulnerability - level 5	Vuln
671787	EulerOS Security Update for expat (EulerOS-SA-2022-1861)	Vulnerability - level 5	Vuln
671788	EulerOS Security Update for bind (EulerOS-SA-2022-1857)	Vulnerability - level 4	Vuln
671789	EulerOS Security Update for golang (EulerOS-SA-2022-1865)	Vulnerability - level 5	Vuln
671794	EulerOS Security Update for libxml2 (EulerOS-SA-2022-1870)	Vulnerability - level 4	Vuln
671796	EulerOS Security Update for expat (EulerOS-SA-2022-1837)	Vulnerability - level 5	Vuln
671800	EulerOS Security Update for httpd (EulerOS-SA-2022-1843)	Vulnerability - level 5	Vuln
671803	EulerOS Security Update for libxml2 (EulerOS-SA-2022-1846)	Vulnerability - level 4	Vuln
671804	EulerOS Security Update for kernel (EulerOS-SA-2022-1844)	Vulnerability - level 4	Vuln
671812	EulerOS Security Update for httpd (EulerOS-SA-2022-1867)	Vulnerability - level 5	Vuln
671816	EulerOS Security Update for bind (EulerOS-SA-2022-1833)	Vulnerability - level 4	Vuln
671817	EulerOS Security Update for kernel (EulerOS-SA-2022-1868)	Vulnerability - level 4	Vuln
671844	EulerOS Security Update for golang (EulerOS-SA-2022-1890)	Vulnerability - level 4	Vuln
671845	EulerOS Security Update for docker-engine (EulerOS-SA-2022-1886)	Vulnerability - level 4	Vuln
671851	EulerOS Security Update for httpd (EulerOS-SA-2022-1893)	Vulnerability - level 5	Vuln
671852	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1909)	Vulnerability - level 5	Vuln
671861	EulerOS Security Update for e2fsprogs (EulerOS-SA-2022-1887)	Vulnerability - level 4	Vuln
671862	EulerOS Security Update for kernel (EulerOS-SA-2022-1896)	Vulnerability - level 4	Vuln
671868	EulerOS Security Update for golang (EulerOS-SA-2022-1930)	Vulnerability - level 4	Vuln
671870	EulerOS Security Update for kernel (EulerOS-SA-2022-1934)	Vulnerability - level 5	Vuln
671874	EulerOS Security Update for bind (EulerOS-SA-2022-1922)	Vulnerability - level 4	Vuln
671881	EulerOS Security Update for docker-engine (EulerOS-SA-2022-1926)	Vulnerability - level 4	Vuln
671890	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1943)	Vulnerability - level 5	Vuln
671896	EulerOS Security Update for compat-openssl10 (EulerOS-SA-2022-1924)	Vulnerability - level 5	Vuln
671915	EulerOS Security Update for kernel (EulerOS-SA-2022-1969)	Vulnerability - level 5	Vuln
671917	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2007)	Vulnerability - level 5	Vuln
671921	EulerOS Security Update for golang (EulerOS-SA-2022-1966)	Vulnerability - level 4	Vuln

671929	EulerOS Security Update for kernel (EulerOS-SA-2022-1999)	Vulnerability - level 4	Vuln
671930	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-1977)	Vulnerability - level 5	Vuln
671962	EulerOS Security Update for golang (EulerOS-SA-2022-1996)	Vulnerability - level 4	Vuln
671975	EulerOS Security Update for kernel (EulerOS-SA-2022-2159)	Vulnerability - level 5	Vuln
671976	EulerOS Security Update for golang (EulerOS-SA-2022-2157)	Vulnerability - level 4	Vuln
671989	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2143)	Vulnerability - level 5	Vuln
671990	EulerOS Security Update for golang (EulerOS-SA-2022-2132)	Vulnerability - level 4	Vuln
672003	EulerOS Security Update for kernel (EulerOS-SA-2022-2134)	Vulnerability - level 4	Vuln
672004	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2168)	Vulnerability - level 5	Vuln
672016	EulerOS Security Update for kernel (EulerOS-SA-2022-2273)	Vulnerability - level 4	Vuln
672017	EulerOS Security Update for kernel (EulerOS-SA-2022-2244)	Vulnerability - level 5	Vuln
672019	EulerOS Security Update for docker-engine (EulerOS-SA-2022-2253)	Vulnerability - level 4	Vuln
672020	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2228)	Vulnerability - level 5	Vuln
672022	EulerOS Security Update for httpd (EulerOS-SA-2022-2256)	Vulnerability - level 5	Vuln
672023	EulerOS Security Update for docker (EulerOS-SA-2022-2265)	Vulnerability - level 4	Vuln
672037	EulerOS Security Update for kernel (EulerOS-SA-2022-2257)	Vulnerability - level 4	Vuln
672041	EulerOS Security Update for httpd (EulerOS-SA-2022-2270)	Vulnerability - level 5	Vuln
672045	EulerOS Security Update for kernel (EulerOS-SA-2022-2225)	Vulnerability - level 5	Vuln
672049	EulerOS Security Update for docker-engine (EulerOS-SA-2022-2240)	Vulnerability - level 4	Vuln
672052	EulerOS Security Update for httpd (EulerOS-SA-2022-2222)	Vulnerability - level 5	Vuln
672054	EulerOS Security Update for compat-openssl (EulerOS-SA-2022-2215)	Vulnerability - level 5	Vuln
672060	EulerOS Security Update for httpd (EulerOS-SA-2022-2243)	Vulnerability - level 5	Vuln
672074	EulerOS Security Update for docker-engine (EulerOS-SA-2022-2218)	Vulnerability - level 4	Vuln
672082	EulerOS Security Update for httpd (EulerOS-SA-2022-2320)	Vulnerability - level 5	Vuln
672086	EulerOS Security Update for kernel (EulerOS-SA-2022-2321)	Vulnerability - level 4	Vuln
672094	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2300)	Vulnerability - level 5	Vuln
672096	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2329)	Vulnerability - level 5	Vuln
672110	EulerOS Security Update for docker-engine (EulerOS-SA-2022-2311)	Vulnerability - level 4	Vuln
672114	EulerOS Security Update for kernel (EulerOS-SA-2022-2292)	Vulnerability - level 4	Vuln
672128	EulerOS Security Update for httpd (EulerOS-SA-2022-2291)	Vulnerability - level 5	Vuln
672139	EulerOS Security Update for kernel (EulerOS-SA-2022-2428)	Vulnerability - level 4	Vuln
672141	EulerOS Security Update for kernel (EulerOS-SA-2022-2441)	Vulnerability - level 4	Vuln
672153	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2446)	Vulnerability - level 5	Vuln
672158	EulerOS Security Update for kernel (EulerOS-SA-2022-2415)	Vulnerability - level 4	Vuln
672162	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2419)	Vulnerability - level 5	Vuln
672172	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2432)	Vulnerability - level 5	Vuln
672193	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2476)	Vulnerability - level 3	Vuln
672205	EulerOS Security Update for kernel (EulerOS-SA-2022-2466)	Vulnerability - level 4	Vuln
672218	EulerOS Security Update for kernel (EulerOS-SA-2022-2619)	Vulnerability - level 4	Vuln
672228	EulerOS Security Update for httpd (EulerOS-SA-2022-2614)	Vulnerability - level 5	Vuln
672242	EulerOS Security Update for e2fsprogs (EulerOS-SA-2022-2600)	Vulnerability - level 4	Vuln
672245	EulerOS Security Update for golang (EulerOS-SA-2022-2610)	Vulnerability - level 4	Vuln
672251	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2022-2629)	Vulnerability - level 5	Vuln

672268	EulerOS Security Update for e2fsprogs (EulerOS-SA-2022-2647)	Vulnerability - level 4	Vuln
672278	EulerOS Security Update for kernel (EulerOS-SA-2022-2686)	Vulnerability - level 4	Vuln
672280	EulerOS Security Update for e2fsprogs (EulerOS-SA-2022-2679)	Vulnerability - level 4	Vuln
672286	EulerOS Security Update for kernel (EulerOS-SA-2022-2654)	Vulnerability - level 4	Vuln
672328	EulerOS Security Update for Open Secure Sockets Layer098e (OpenSSL098e) (EulerOS-SA-2022-2717)	Vulnerability - level 4	Vuln
672329	EulerOS Security Update for dhcp (EulerOS-SA-2022-2759)	Vulnerability - level 4	Vuln
672354	EulerOS Security Update for kernel (EulerOS-SA-2022-2732)	Vulnerability - level 4	Vuln
672358	EulerOS Security Update for dhcp (EulerOS-SA-2022-2724)	Vulnerability - level 4	Vuln
672376	EulerOS Security Update for deltarpm (EulerOS-SA-2022-2723)	Vulnerability - level 5	Vuln
672379	EulerOS Security Update for deltarpm (EulerOS-SA-2022-2758)	Vulnerability - level 5	Vuln
672391	EulerOS Security Update for kernel (EulerOS-SA-2022-2767)	Vulnerability - level 4	Vuln
672424	EulerOS Security Update for dhcp (EulerOS-SA-2022-2842)	Vulnerability - level 4	Vuln
672438	EulerOS Security Update for deltarpm (EulerOS-SA-2022-2841)	Vulnerability - level 5	Vuln
672447	EulerOS Security Update for linux-sgx (EulerOS-SA-2022-2852)	Vulnerability - level 5	Vuln
672461	EulerOS Security Update for dhcp (EulerOS-SA-2022-2817)	Vulnerability - level 4	Vuln
672469	EulerOS Security Update for deltarpm (EulerOS-SA-2022-2816)	Vulnerability - level 5	Vuln
672474	EulerOS Security Update for kernel (EulerOS-SA-2022-2823)	Vulnerability - level 4	Vuln
672477	EulerOS Security Update for dhcp (EulerOS-SA-2023-1032)	Vulnerability - level 4	Vuln
672510	EulerOS Security Update for dhcp (EulerOS-SA-2023-1007)	Vulnerability - level 4	Vuln
672653	EulerOS Security Update for kernel (EulerOS-SA-2023-1388)	Vulnerability - level 4	Vuln
672656	EulerOS Security Update for grub2 (EulerOS-SA-2023-1386)	Vulnerability - level 4	Vuln
672662	EulerOS Security Update for grub2 (EulerOS-SA-2023-1358)	Vulnerability - level 4	Vuln
672683	EulerOS Security Update for httpd (EulerOS-SA-2023-1408)	Vulnerability - level 5	Vuln
672691	EulerOS Security Update for httpd (EulerOS-SA-2023-1423)	Vulnerability - level 5	Vuln
672706	EulerOS Security Update for e2fsprogs (EulerOS-SA-2023-1439)	Vulnerability - level 4	Vuln
672732	EulerOS Security Update for e2fsprogs (EulerOS-SA-2023-1464)	Vulnerability - level 4	Vuln
672878	EulerOS Security Update for e2fsprogs (EulerOS-SA-2023-1592)	Vulnerability - level 4	Vuln
672879	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1602)	Vulnerability - level 4	Vuln
672970	EulerOS Security Update for shim (EulerOS-SA-2023-1853)	Vulnerability - level 4	Vuln
672980	EulerOS Security Update for shim (EulerOS-SA-2023-1878)	Vulnerability - level 4	Vuln
672984	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1875)	Vulnerability - level 4	Vuln
673006	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1850)	Vulnerability - level 4	Vuln
673018	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1982)	Vulnerability - level 4	Vuln
673033	EulerOS Security Update for shim (EulerOS-SA-2023-1984)	Vulnerability - level 4	Vuln
673041	EulerOS Security Update for open-iscsi (EulerOS-SA-2023-1980)	Vulnerability - level 4	Vuln
673042	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-1960)	Vulnerability - level 4	Vuln
673044	EulerOS Security Update for shim (EulerOS-SA-2023-1962)	Vulnerability - level 4	Vuln
673050	EulerOS Security Update for open-iscsi (EulerOS-SA-2023-1958)	Vulnerability - level 4	Vuln
673060	EulerOS Security Update for shim-signed (EulerOS-SA-2023-2170)	Vulnerability - level 4	Vuln
673064	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2161)	Vulnerability - level 4	Vuln
673072	EulerOS Security Update for shim (EulerOS-SA-2023-2169)	Vulnerability - level 4	Vuln
673085	EulerOS Security Update for expat (EulerOS-SA-2023-2143)	Vulnerability - level 5	Vuln
673086	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL)111d (EulerOS-SA-2023-2162)	Vulnerability - level 5	Vuln
673098	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL)111d (EulerOS-SA-2023-2183)	Vulnerability - level 3	Vuln
673136	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2299)	Vulnerability - level 4	Vuln
673145	EulerOS Security Update for shim (EulerOS-SA-2023-2301)	Vulnerability - level 4	Vuln
673151	EulerOS Security Update for shim (EulerOS-SA-2023-2277)	Vulnerability - level 4	Vuln
673156	EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2023-2275)	Vulnerability - level 4	Vuln

68528	Multiple Microsoft Windows RPC/DCOM Vulnerabilities (MS04-012)	Vulnerability - level 5	Practice
690025	Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (882a38f9-17dd-11ec-b335-d4c9ef517024)	Vulnerability - level 4	Vuln
690030	Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (7062bce0-1b17-11ec-9d9d-0022489ad614)	Vulnerability - level 3	Vuln
690032	Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (b092bd4f-1b16-11ec-9d9d-0022489ad614)	Vulnerability - level 4	Vuln
690033	Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (f53dab71-1b15-11ec-9d9d-0022489ad614)	Vulnerability - level 3	Vuln
690040	Free Berkeley Software Distribution (FreeBSD) Security Update for go (4ea1082a-1259-11ec-b4fa-dd5a552bdd17)	Vulnerability - level 3	Vuln
690055	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (96811d4a-04ec-11ec-9b84-d4c9ef517024)	Vulnerability - level 4	Vuln
690066	Free Berkeley Software Distribution (FreeBSD) Security Update for go (880552c4-f63f-11eb-9d56-7186043316e9)	Vulnerability - level 2	Vuln
690068	Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (38a4a043-e937-11eb-9b84-d4c9ef517024)	Vulnerability - level 4	Vuln
690107	Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (cce76eca-ca16-11eb-9b84-d4c9ef517024)	Vulnerability - level 4	Vuln
690134	Free Berkeley Software Distribution (FreeBSD) Security Update for libxml2 (524bd03a-bb75-11eb-bf35-080027f515ea)	Vulnerability - level 2	Vuln
690151	Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (56ba4513-a1be-11eb-9072-d4c9ef517024)	Vulnerability - level 3	Vuln
690183	Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (c0c1834c-9761-11eb-acfd-0022489ad614)	Vulnerability - level 4	Vuln
690185	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (5a668ab3-8d86-11eb-b8d6-d4c9ef517024)	Vulnerability - level 3	Vuln
690192	Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (c9387e4d-2f5f-11ec-8be6-d4c9ef517024)	Vulnerability - level 4	Vuln
690211	Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (2f3cd69e-7dee-11eb-b92e-0022489ad614)	Vulnerability - level 3	Vuln
690227	Free Berkeley Software Distribution (FreeBSD) Security Update for go (930def19-3e05-11ec-9ba8-002324b2fba8)	Vulnerability - level 2	Vuln
690292	Free Berkeley Software Distribution (FreeBSD) Security Update for FreeBSD (7cfcea05-600a-11e6-a6c3-14dae9d210b8)	Vulnerability - level 3	Vuln
690300	Free Berkeley Software Distribution (FreeBSD) Security Update for openssh (2920c449-4850-11e5-825f-c80aa9043978)	Vulnerability - level 4	Vuln
690301	Free Berkeley Software Distribution (FreeBSD) Security Update for mercurial (b0628e53-092a-4037-938b-29805a7cd31b)	Vulnerability - level 5	Vuln
690305	Free Berkeley Software Distribution (FreeBSD) Security Update for freeimage (33459061-a1d6-11e5-8794-bcaec565249c)	Vulnerability - level 3	Vuln
690327	Free Berkeley Software Distribution (FreeBSD) Security Update for krb5 (e3f64457-cccd-11e2-af76-206a8a720317)	Vulnerability - level 3	Vuln
690340	Free Berkeley Software Distribution (FreeBSD) Security Update for trafficserver (6318b303-3507-11e4-b76c-0011d823eebd)	Vulnerability - level 5	Vuln
690348	Free Berkeley Software Distribution (FreeBSD) Security Update for curl (3c77f139-3a09-11eb-929d-d4c9ef517024)	Vulnerability - level 3	Vuln
690390	Free Berkeley Software Distribution (FreeBSD) Security Update for intel cpu issues (fbcba194-ac7d-11ea-8b5e-b42e99a1b9c3)	Vulnerability - level 2	Vuln
690397	Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (08b553ed-537a-11eb-be6e-0022489ad614)	Vulnerability - level 3	Vuln
690403	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (1d56cfc5-3970-11eb-929d-d4c9ef517024)	Vulnerability - level 2	Vuln
690442	Free Berkeley Software Distribution (FreeBSD) Security Update for dnsmasq (5b5cf6e5-5b51-11eb-95ac-7f9491278677)	Vulnerability - level 4	Vuln

690499	Free Berkeley Software Distribution (FreeBSD) Security Update for libxml (f5abafc0-fcf6-11ea-8758-e0d55e2a8bf9)	Vulnerability - level 3	Vuln
690520	Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (4ca5894c-f7f1-11ea-8ff8-0022489ad614)	Vulnerability - level 3	Vuln
690551	Free Berkeley Software Distribution (FreeBSD) Security Update for apache (c84dc9ad-41f7-11dd-a4f9-00163e000016)	Vulnerability - level 3	Vuln
690588	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (c82ecac5-6e3f-11e8-8777-b499baebfeaf)	Vulnerability - level 3	Vuln
690650	Free Berkeley Software Distribution (FreeBSD) Security Update for quagga (e15a22ce-f16f-446b-9ca7-6859350c2e75)	Vulnerability - level 4	Vuln
690735	Free Berkeley Software Distribution (FreeBSD) Security Update for go (720505fe-593f-11ec-9ba8-002324b2fba8)	Vulnerability - level 3	Vuln
690776	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (1aaaa5c6-804d-11ec-8be6-d4c9ef517024)	Vulnerability - level 3	Vuln
690780	Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (7262f826-795e-11ec-8be6-d4c9ef517024)	Vulnerability - level 4	Vuln
690812	Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (6601c08d-a46c-11ec-8be6-d4c9ef517024)	Vulnerability - level 4	Vuln
690816	Free Berkeley Software Distribution (FreeBSD) Security Update for freebsd-kernel (8d20bd48-a4f3-11ec-90de-1c697aa5a594)	Vulnerability - level 3	Vuln
690817	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Virtual Private Network (OpenVPN) (45a72180-a640-11ec-a08b-85298243e224)	Vulnerability - level 4	Vuln
690818	Free Berkeley Software Distribution (FreeBSD) Security Update for go (e2af876f-a7c8-11ec-9a2a-002324b2fba8)	Vulnerability - level 4	Vuln
690861	Free Berkeley Software Distribution (FreeBSD) Security Update for go (61bce714-ca0c-11ec-9cfc-10c37b4ac2ea)	Vulnerability - level 4	Vuln
690862	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (fceb2b08-cb76-11ec-a06f-d4c9ef517024)	Vulnerability - level 4	Vuln
690875	Free Berkeley Software Distribution (FreeBSD) Security Update for e2fsprogs (a58f3fde-e4e0-11ec-8340-2d623369b8b5)	Vulnerability - level 4	Vuln
690877	Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (49adfbe5-e7d1-11ec-8fbd-d4c9ef517024)	Vulnerability - level 4	Vuln
690881	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (4eeb93bf-f204-11ec-8fbd-d4c9ef517024)	Vulnerability - level 4	Vuln
690892	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (a28e8b7e-fc70-11ec-856e-d4c9ef517024)	Vulnerability - level 4	Vuln
690894	Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (b9210706-feb0-11ec-81fa-1c697a616631)	Vulnerability - level 4	Vuln
690902	Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (8e150606-08c9-11ed-856e-d4c9ef517024)	Vulnerability - level 5	Vuln
690971	Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (4b9c1c17-587c-11ed-856e-d4c9ef517024)	Vulnerability - level 4	Vuln
691051	Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (648a432c-a71f-11ed-86e9-d4c9ef517024)	Vulnerability - level 4	Vuln
691110	Free Berkeley Software Distribution (FreeBSD) Security Update for samba (e86b8e4d-d551-11ed-8d1e-005056a311d1)	Vulnerability - level 3	Vuln
691113	Free Berkeley Software Distribution (FreeBSD) Security Update for py39 (3f6d6181-79b2-4d33-bb1e-5d3f9df0c1d1)	Vulnerability - level 2	Vuln
691136	Free Berkeley Software Distribution (FreeBSD) Security Update for py (c1a8ed1c-2814-4260-82aa-9e37c83aac93)	Vulnerability - level 4	Vuln
691183	Free Berkeley Software Distribution (FreeBSD) Security Update for python (d86becfe-05a4-11ee-9d4a-080027eda32c)	Vulnerability - level 4	Vuln

70046	Samba NMBD Logon Request Remote Buffer Overflow Vulnerability	Vulnerability - level 4	Practice
70050	Samba NSS_Info Plugin Local Privilege Escalation Vulnerability	Vulnerability - level 4	Practice
710009	Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202103-03)	Vulnerability - level 3	Vuln
710015	Gentoo Linux GRUB Multiple Vulnerabilities (GLSA 202104-05)	Vulnerability - level 4	Vuln
710030	Gentoo Linux Apache Multiple vulnerabilities (GLSA 202107-38)	Vulnerability - level 2	Vuln
710049	Gentoo Linux Apache Commons FileUpload Multiple Vulnerabilities (GLSA 202107-39)	Vulnerability - level 3	Vuln
710071	Gentoo Linux libxml2 Multiple vulnerabilities (GLSA 202107-05)	Vulnerability - level 2	Vuln
710119	Gentoo Linux Open Secure Sockets Layer Multiple Vulnerabilities (GLSA 201911-04)	Vulnerability - level 2	Vuln
710154	Gentoo Linux LibVNCServer Multiple vulnerabilities (GLSA 201908-05)	Vulnerability - level 3	Vuln
710197	Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201903-03)	Vulnerability - level 3	Vuln
710242	Gentoo Linux Quagga Multiple Vulnerabilities (GLSA 201804-17)	Vulnerability - level 4	Vuln
710274	Gentoo Linux OpenSSH Permission issue Vulnerability (GLSA 201801-05)	Vulnerability - level 3	Vuln
710295	Gentoo Linux Open Secure Sockets Layer Denial of service Vulnerability (GLSA 201811-03)	Vulnerability - level 3	Vuln
710321	Gentoo Linux hostapd and wpa_supplicant Key Reinstallation Vulnerability (GLSA 201711-03)	Vulnerability - level 3	Vuln
710347	Gentoo Linux Oracle Java Development Toolkit/Java Runtime Error, IcedTea Multiple Vulnerabilities (GLSA 201709-22)	Vulnerability - level 3	Vuln
710380	Gentoo Linux Pidgin Arbitrary code execution Vulnerability (GLSA 201706-10)	Vulnerability - level 3	Vuln
710385	Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201701-47)	Vulnerability - level 3	Vuln
710455	Gentoo Linux FreedImage Multiple Vulnerabilities (GLSA 201701-68)	Vulnerability - level 3	Vuln
710461	Gentoo Linux Apache Multiple Vulnerabilities (GLSA 201701-36)	Vulnerability - level 3	Vuln
710479	Gentoo Linux libTIFF Multiple Vulnerabilities (GLSA 201701-16)	Vulnerability - level 3	Vuln
710507	Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 201712-03)	Vulnerability - level 3	Vuln
710518	Gentoo Linux Mozilla Network Security Service (NSS) Multiple Vulnerabilities (GLSA 201701-46)	Vulnerability - level 3	Vuln
710521	Gentoo Linux Mercurial Multiple Vulnerabilities (GLSA 201709-18)	Vulnerability - level 5	Vuln
710523	Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 201704-01)	Vulnerability - level 4	Vuln
710532	Gentoo Linux T1Lib Vulnerability (GLSA 201701-57)	Vulnerability - level 3	Vuln
710584	Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)	Vulnerability - level 5	Vuln
710595	Gentoo Linux Apache HTTPD Multiple Vulnerabilities (GLSA 202208-20)	Vulnerability - level 5	Vuln
710616	Gentoo Linux IBM Spectrum Protect Multiple Vulnerabilities (GLSA 202209-02)	Vulnerability - level 5	Vuln
710626	Gentoo Linux Expat Multiple Vulnerabilities (GLSA 202209-24)	Vulnerability - level 5	Vuln
710638	Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202210-02)	Vulnerability - level 5	Vuln
710642	Gentoo Linux libxml2 Multiple Vulnerabilities (GLSA 202210-03)	Vulnerability - level 4	Vuln
710661	Gentoo Linux ISC BIND Multiple Vulnerabilities (GLSA 202210-25)	Vulnerability - level 4	Vuln
710683	Gentoo Linux PostgreSQL Multiple Vulnerabilities (GLSA 202211-04)	Vulnerability - level 4	Vuln
710702	Gentoo Linux Mbed Transport Layer Security (TLS) Multiple Vulnerabilities (GLSA 202301-08)	Vulnerability - level 5	Vuln
730031	IBM MQ Appliance Multiple Vulnerabilities(6403297)	Vulnerability - level 3	Vuln
730068	HPE Integrated Lights-Out (iLO) Remote Memory Corruption Vulnerability (hpesbhf04106)	Vulnerability - level 4	Vuln
730109	Apache HTTP Server Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
730118	Dell Unisphere for PowerMax Security Update for Multiple Third-Party Component Vulnerabilities	Vulnerability - level 3	Vuln

730119	Dell Solutions Enabler Security Update for Multiple Third-Party Component Vulnerabilities	Vulnerability - level 3	Vuln
730121	McAfee Web Gateway Multiple Vulnerabilities (WP-3484,WP-3744,WP-3745,WP-3746,WP-3747,WP-3793,WP-3800)	Vulnerability - level 3	Vuln
730135	Cisco Prime Infrastructure Denial of Service (DoS) Vulnerability in Open Secure Sockets Layer (OpenSSL) Affecting Cisco Products (cisco-sa-openssl-2021-GHY28dJd)	Potential Vulnerability - level 3	Practice
730155	McAfee Web Gateway Multiple Vulnerabilities(WP-3580, WP-3656, WP-3815, WP-3878, WP-3882, WP-3934,WP-3935, WP-3936, WP-3999)	Vulnerability - level 4	Vuln
730206	McAfee Web Gateway Multiple Vulnerabilities (WP-3792, WP-4003, WP-4021, WP-4058, WP-4067)	Vulnerability - level 4	Vuln
730209	Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
730228	McAfee Web Gateway Multiple Vulnerabilities (WP-3445, WP-3483, WP-3527, WP-3528, WP-3547, WP-3584,WP-3589,WP-3611)	Vulnerability - level 3	Vuln
730272	McAfee Web Gateway Multiple Vulnerabilities (WP-3806,WP-4203,WP-3710,WP-4073,WP-3663,WP-4158,WP-4164,WP-3247)	Vulnerability - level 3	Vuln
730310	Splunk Enterprise and Light Denial of Service (DoS) Vulnerability (SP-CAAAPSV) (SPL-129207)	Vulnerability - level 5	Vuln
730319	Palo Alto Networks (PAN-OS) Impact of the Raccoon Attack Vulnerability (PAN-154936)	Potential Vulnerability - level 2	Practice
730371	McAfee Web Gateway Multiple Vulnerabilities (WP-3335,WP-4131,WP-4159,WP-4237,WP-4259,WP-4329,WP-4348,WP-4355,WP-4376,WP-4407,WP-4421)	Vulnerability - level 5	Vuln
730403	Apache Hypertext Transfer Protocol (HTTP) Server Out-of-bounds Write Vulnerability	Potential Vulnerability - level 4	Practice
730444	Atlassian Jira Server and Data Center Regular Expression Denial of Service (ReDoS) Vulnerability (JRASERVER-73244)	Vulnerability - level 4	Vuln
730529	Apache Hypertext Transfer Protocol Server (HTTP Server) mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism Vulnerability	Potential Vulnerability - level 5	Practice
730739	IBM Aspera Faspex Multiple Security Vulnerabilities (6952319)	Vulnerability - level 5	Vuln
730818	IBM MQ Appliance Multiple Security Vulnerabilities (6986567)	Vulnerability - level 3	Vuln
74213	McAfee Webshield SMTP Remote Format String Vulnerability	Vulnerability - level 4	Vuln
74258	IBM Lotus Domino HTTP Response Splitting and Cross-Site Scripting Vulnerabilities	Potential Vulnerability - level 3	Practice
74273	IBM Lotus Domino Multiple Vulnerabilities	Vulnerability - level 5	Practice
750027	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2021:1658-1)	Vulnerability - level 3	Vuln
750047	SUSE Enterprise Linux Security Update for postgresql10 (SUSE-SU-2021:1782-1)	Vulnerability - level 3	Vuln
750050	SUSE Enterprise Linux Security Update for postgresql13 (SUSE-SU-2021:1784-1)	Vulnerability - level 3	Vuln
750053	SUSE Enterprise Linux Security Update for postgresql12 (SUSE-SU-2021:1783-1)	Vulnerability - level 3	Vuln
750055	SUSE Enterprise Linux Security Update for curl (SUSE-SU-2021:1786-1)	Vulnerability - level 3	Vuln
750117	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1891-1)	Vulnerability - level 4	Vuln
750125	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1887-1)	Vulnerability - level 4	Vuln
750139	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1913-1)	Vulnerability - level 4	Vuln
750140	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1912-1)	Vulnerability - level 4	Vuln
750142	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2021:1929-1)	Vulnerability - level 4	Vuln

750145	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2021:1932-1)	Vulnerability - level 4	Vuln
750146	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2021:1931-1)	Vulnerability - level 4	Vuln
750147	SUSE Enterprise Linux Security Update for ucode-intel (SUSE-SU-2021:1930-1)	Vulnerability - level 4	Vuln
750171	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0843-1)	Vulnerability - level 4	Vuln
750201	OpenSUSE Security Update for libxml2 (openSUSE-SU-2021:0764-1)	Vulnerability - level 4	Vuln
750222	OpenSUSE Security Update for libxml2 (openSUSE-SU-2021:0692-1)	Vulnerability - level 3	Vuln
750231	OpenSUSE Security Update for bind (openSUSE-SU-2021:0668-1)	Vulnerability - level 4	Vuln
750293	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (openSUSE-SU-2021:0476-1)	Vulnerability - level 4	Vuln
750297	OpenSUSE Security Update for nghttp2 (openSUSE-SU-2021:0468-1)	Vulnerability - level 4	Vuln
750300	OpenSUSE Security Update for grub2 (openSUSE-SU-2021:0462-1)	Vulnerability - level 4	Vuln
750308	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (openSUSE-SU-2021:0430-1)	Vulnerability - level 3	Vuln
750310	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (openSUSE-SU-2021:0427-1)	Vulnerability - level 3	Vuln
750317	OpenSUSE Security Update for openldap2 (openSUSE-SU-2021:0408-1)	Vulnerability - level 4	Vuln
750333	OpenSUSE Security Update for bind (openSUSE-SU-2021:0375-1)	Vulnerability - level 4	Vuln
750335	OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:0372-1)	Vulnerability - level 4	Vuln
750339	OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:0356-1)	Vulnerability - level 4	Vuln
750340	OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:0357-1)	Vulnerability - level 4	Vuln
750374	OpenSUSE Security Update for openvswitch (openSUSE-SU-2021:0239-1)	Vulnerability - level 4	Vuln
750376	OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)	Vulnerability - level 3	Vuln
750407	OpenSUSE Security Update for dnsmasq (openSUSE-SU-2021:0129-1)	Vulnerability - level 4	Vuln
750409	OpenSUSE Security Update for dnsmasq (openSUSE-SU-2021:0124-1)	Vulnerability - level 4	Vuln
750412	OpenSUSE Security Update for openldap2 (openSUSE-SU-2021:0107-1)	Vulnerability - level 3	Vuln
750414	OpenSUSE Security Update for openldap2 (openSUSE-SU-2021:0102-1)	Vulnerability - level 3	Vuln
750420	OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:0082-1)	Vulnerability - level 3	Vuln
750431	OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:0065-1)	Vulnerability - level 3	Vuln
750432	OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:0064-1)	Vulnerability - level 3	Vuln
750484	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (openSUSE-SU-2020:2269-1)	Vulnerability - level 4	Vuln
750488	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2260-1)	Vulnerability - level 4	Vuln
750490	OpenSUSE Security Update for curl (openSUSE-SU-2020:2249-1)	Vulnerability - level 3	Vuln

750491	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (openSUSE-SU-2020:2245-1)	Vulnerability - level 4	Vuln
750492	OpenSUSE Security Update for curl (openSUSE-SU-2020:2238-1)	Vulnerability - level 3	Vuln
750495	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (openSUSE-SU-2020:2236-1)	Vulnerability - level 4	Vuln
750498	Open Software and Systems Development (OpenSUSE) Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (openSUSE-SU-2020:2223-1)	Vulnerability - level 4	Vuln
750518	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2161-1)	Vulnerability - level 4	Vuln
750533	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2112-1)	Vulnerability - level 4	Vuln
750537	OpenSUSE Security Update for ucode-intel (openSUSE-SU-2020:2098-1)	Vulnerability - level 4	Vuln
750548	OpenSUSE Security Update for ucode-intel (openSUSE-SU-2020:2075-1)	Vulnerability - level 4	Vuln
750549	OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2020:2059-1)	Vulnerability - level 3	Vuln
750557	OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2020:2053-1)	Vulnerability - level 3	Vuln
750568	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2034-1)	Vulnerability - level 4	Vuln
750595	OpenSUSE Security Update for u-boot (openSUSE-SU-2020:1930-1)	Vulnerability - level 4	Vuln
750598	OpenSUSE Security Update for ucode-intel (openSUSE-SU-2020:1923-1)	Vulnerability - level 3	Vuln
750600	OpenSUSE Security Update for openldap2 (openSUSE-SU-2020:1918-1)	Vulnerability - level 4	Vuln
750602	OpenSUSE Security Update for openldap2 (openSUSE-SU-2020:1920-1)	Vulnerability - level 4	Vuln
750604	OpenSUSE Security Update for ucode-intel (openSUSE-SU-2020:1915-1)	Vulnerability - level 3	Vuln
750609	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:1906-1)	Vulnerability - level 4	Vuln
750638	OpenSUSE Security Update for postgresql10 (openSUSE-SU-2021:0894-1)	Vulnerability - level 3	Vuln
750642	OpenSUSE Security Update for libxml2 (openSUSE-SU-2021:0886-1)	Vulnerability - level 3	Vuln
750645	OpenSUSE Security Update for ucode-intel (openSUSE-SU-2021:0876-1)	Vulnerability - level 4	Vuln
750660	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2021:2004-1)	Vulnerability - level 4	Vuln
750662	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2021:2006-1)	Vulnerability - level 4	Vuln
750677	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2021:2016-1)	Vulnerability - level 3	Vuln
750690	Software and Systems Development (SUSE) Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (SUSE-SU-2020:3762-1)	Vulnerability - level 4	Vuln
750719	OpenSUSE Security Update for apache2 (openSUSE-SU-2021:0908-1)	Vulnerability - level 4	Vuln
750738	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3326-1)	Vulnerability - level 3	Vuln
750741	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0947-1)	Vulnerability - level 4	Vuln
750762	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)	Vulnerability - level 4	Vuln

750766	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)	Vulnerability - level 4	Vuln
750770	OpenSUSE Security Update for libxml2 (openSUSE-SU-2021:1917-1)	Vulnerability - level 3	Vuln
750776	OpenSUSE Security Update for postgresql13 (openSUSE-SU-2021:1785-1)	Vulnerability - level 3	Vuln
750804	OpenSUSE Security Update for bind (openSUSE-SU-2021:1826-1)	Vulnerability - level 4	Vuln
750808	OpenSUSE Security Update for postgresql10 (openSUSE-SU-2021:1970-1)	Vulnerability - level 3	Vuln
750813	OpenSUSE Security Update for apache2 (openSUSE-SU-2021:2127-1)	Vulnerability - level 4	Vuln
750816	OpenSUSE Security Update for postgresql12 (openSUSE-SU-2021:1994-1)	Vulnerability - level 3	Vuln
750817	OpenSUSE Security Update for ucode-intel (openSUSE-SU-2021:1933-1)	Vulnerability - level 4	Vuln
750831	SUSE Enterprise Linux Security Update for sqlite3 (SUSE-SU-2021:2320-1)	Vulnerability - level 4	Vuln
750833	OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:2327-1)	Vulnerability - level 4	Vuln
750834	OpenSUSE Security Update for sqlite3 (openSUSE-SU-2021:2320-1)	Vulnerability - level 4	Vuln
750837	SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2021:2353-1)	Vulnerability - level 4	Vuln
750840	OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:2353-1)	Vulnerability - level 4	Vuln
750856	OpenSUSE Security Update for sqlite3 (openSUSE-SU-2021:1058-1)	Vulnerability - level 4	Vuln
750858	OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:1061-1)	Vulnerability - level 4	Vuln
750859	OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:1059-1)	Vulnerability - level 4	Vuln
750864	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2421-1)	Vulnerability - level 4	Vuln
750880	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2451-1)	Vulnerability - level 4	Vuln
750982	SUSE Enterprise Linux Security Update for postgresql10 (SUSE-SU-2021:2777-1)	Vulnerability - level 3	Vuln
750986	SUSE Enterprise Linux Security Update for go1.15 (SUSE-SU-2021:2787-1)	Vulnerability - level 3	Vuln
750993	SUSE Enterprise Linux Security Update for nodejs8 (SUSE-SU-2021:2790-1)	Vulnerability - level 4	Vuln
751012	OpenSUSE Security Update for go1.15 (openSUSE-SU-2021:2787-1)	Vulnerability - level 3	Vuln
751017	OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:2788-1)	Vulnerability - level 3	Vuln
751027	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2021:2831-1)	Vulnerability - level 4	Vuln
751028	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2021:2829-1)	Vulnerability - level 4	Vuln
751029	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2021:2826-1)	Vulnerability - level 4	Vuln
751030	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2021:2827-1)	Vulnerability - level 4	Vuln
751031	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2021:2833-1)	Vulnerability - level 4	Vuln
751032	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2021:2825-1)	Vulnerability - level 4	Vuln
751034	OpenSUSE Security Update for openssl-1_0_0 (openSUSE-SU-2021:2827-1)	Vulnerability - level 4	Vuln
751035	OpenSUSE Security Update for openssl-1_1 (openSUSE-SU-2021:2830-1)	Vulnerability - level 4	Vuln

751041	OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:1199-1)	Vulnerability - level 3	Vuln
751049	OpenSUSE Security Update for Open Secure Sockets Layer (OpenSSL) (openSUSE-SU-2021:1189-1)	Vulnerability - level 4	Vuln
751050	OpenSUSE Security Update for Open Secure Sockets Layer (OpenSSL) (openSUSE-SU-2021:1188-1)	Vulnerability - level 4	Vuln
751059	SUSE Enterprise Linux Security Update for compat- Open Secure Sockets Layer (openssl098) (SUSE-SU-2021:2852-1)	Vulnerability - level 4	Vuln
751061	OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:2875-1)	Vulnerability - level 4	Vuln
751066	OpenSUSE Security Update for go1.15 (openSUSE-SU-2021:1207-1)	Vulnerability - level 3	Vuln
751071	OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:1214-1)	Vulnerability - level 4	Vuln
751093	OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:2953-1)	Vulnerability - level 3	Vuln
751106	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer-1_1 (openssl-1_1) (SUSE-SU-2021:2967-1)	Vulnerability - level 2	Vuln
751108	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer-1_1 (openssl-1_1) (SUSE-SU-2021:2968-1)	Vulnerability - level 2	Vuln
751112	OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:1239-1)	Vulnerability - level 3	Vuln
751116	OpenSUSE Security Update for Open Secure Sockets Layer-1_1 (openssl-1_1) (openSUSE-SU-2021:2966-1)	Vulnerability - level 2	Vuln
751118	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer-1_1 (OpenSSL-1_1) (SUSE-SU-2021:2996-1)	Vulnerability - level 2	Vuln
751119	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer-1_0_0 (OpenSSL-1_0_0) (SUSE-SU-2021:2994-1)	Vulnerability - level 2	Vuln
751122	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer-1_0_0 (SUSE-SU-2021:2995-1)	Vulnerability - level 2	Vuln
751123	OpenSUSE Security Update for Open Secure Sockets Layer-1_1 (OpenSSL-1_1) (openSUSE-SU-2021:1248-1)	Vulnerability - level 2	Vuln
751125	OpenSUSE Security Update for Open Secure Sockets Layer-1_0_0 (OpenSSL-1_0_0) (openSUSE-SU-2021:2994-1)	Vulnerability - level 2	Vuln
751128	SUSE Enterprise Linux Security Update for compat-Open Secure Sockets Layer098 (OpenSSL098) (SUSE-SU-2021:3019-1)	Vulnerability - level 2	Vuln
751129	OpenSUSE Security Update for Open Secure Sockets Layer-1_0_0 (OpenSSL-1_0_0) (openSUSE-SU-2021:1261-1)	Vulnerability - level 2	Vuln
751152	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2021:3144-1)	Vulnerability - level 2	Vuln
751168	SUSE Enterprise Linux Security Update for sqlite3 (SUSE-SU-2021:3215-1)	Vulnerability - level 4	Vuln
751171	OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:3211-1)	Vulnerability - level 4	Vuln
751178	OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:1313-1)	Vulnerability - level 4	Vuln
751198	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2021:3299-1)	Vulnerability - level 4	Vuln
751202	OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:3292-1)	Vulnerability - level 4	Vuln
751204	OpenSUSE Security Update for nodejs8 (openSUSE-SU-2021:3294-1)	Vulnerability - level 4	Vuln
751216	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2021:3335-1)	Vulnerability - level 4	Vuln
751228	OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:1342-1)	Vulnerability - level 4	Vuln
751229	OpenSUSE Security Update for nodejs8 (openSUSE-SU-2021:1343-1)	Vulnerability - level 4	Vuln
751264	SUSE Enterprise Linux Security Update for postgresql10 (SUSE-SU-2021:3481-1)	Vulnerability - level 4	Vuln
751272	SUSE Enterprise Linux Security Update for containerd, docker, runc (SUSE-SU-2021:3506-1)	Vulnerability - level 4	Vuln

751273	OpenSUSE Security Update for containerd, docker, runc (openSUSE-SU-2021:3506-1)	Vulnerability - level 4	Vuln
751279	OpenSUSE Security Update for apache2 (openSUSE-SU-2021:3522-1)	Vulnerability - level 4	Vuln
751303	OpenSUSE Security Update for containerd, docker, runc (openSUSE-SU-2021:1404-1)	Vulnerability - level 4	Vuln
751314	OpenSUSE Security Update for apache2 (openSUSE-SU-2021:1438-1)	Vulnerability - level 4	Vuln
751363	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:3657-1)	Vulnerability - level 4	Vuln
751396	OpenSUSE Security Update for bind (openSUSE-SU-2021:3773-1)	Vulnerability - level 4	Vuln
751400	OpenSUSE Security Update for bind (openSUSE-SU-2021:1502-1)	Vulnerability - level 4	Vuln
751425	OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:3834-1)	Vulnerability - level 3	Vuln
751431	OpenSUSE Security Update for go1.17 (openSUSE-SU-2021:3833-1)	Vulnerability - level 3	Vuln
751457	OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:3940-1)	Vulnerability - level 4	Vuln
751461	OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:1539-1)	Vulnerability - level 3	Vuln
751475	OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:3964-1)	Vulnerability - level 4	Vuln
751509	OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:1574-1)	Vulnerability - level 4	Vuln
751518	OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:1552-1)	Vulnerability - level 4	Vuln
751547	SUSE Enterprise Linux Security Update for go1.16 (SUSE-SU-2021:4169-1)	Vulnerability - level 3	Vuln
751549	SUSE Enterprise Linux Security Update for go1.17 (SUSE-SU-2021:4186-1)	Vulnerability - level 3	Vuln
751553	OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:4169-1)	Vulnerability - level 3	Vuln
751554	OpenSUSE Security Update for go1.17 (openSUSE-SU-2021:4186-1)	Vulnerability - level 3	Vuln
751559	OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:1626-1)	Vulnerability - level 3	Vuln
751624	SUSE Enterprise Linux Security Update for busybox (SUSE-SU-2022:0135-1)	Vulnerability - level 5	Vuln
751633	OpenSUSE Security Update for busybox (openSUSE-SU-2022:0135-1)	Vulnerability - level 5	Vuln
751635	OpenSUSE Security Update for bind (openSUSE-SU-2022:0151-1)	Vulnerability - level 3	Vuln
751651	SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0178-1)	Vulnerability - level 5	Vuln
751653	SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0179-1)	Vulnerability - level 5	Vuln
751662	OpenSUSE Security Update for expat (openSUSE-SU-2022:0178-1)	Vulnerability - level 5	Vuln
751692	OpenSUSE Security Update for containerd, docker (openSUSE-SU-2022:0334-1)	Vulnerability - level 4	Vuln
751724	SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0495-1)	Vulnerability - level 5	Vuln
751730	SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0498-1)	Vulnerability - level 5	Vuln
751731	SUSE Enterprise Linux Security Update for wpa_supplicant (SUSE-SU-2022:0504-1)	Vulnerability - level 5	Vuln
751741	OpenSUSE Security Update for expat (openSUSE-SU-2022:0498-1)	Vulnerability - level 5	Vuln
751759	SUSE Enterprise Linux Security Update for nodejs8 (SUSE-SU-2022:0563-1)	Vulnerability - level 5	Vuln
751773	SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2022:0657-1)	Vulnerability - level 5	Vuln
751781	OpenSUSE Security Update for nodejs12 (openSUSE-SU-2022:0657-1)	Vulnerability - level 5	Vuln
751782	SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0698-1)	Vulnerability - level 5	Vuln
751783	SUSE Enterprise Linux Security Update for nodejs8 (SUSE-SU-2022:0704-1)	Vulnerability - level 5	Vuln

751795	SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0713-1)	Vulnerability - level 5	Vuln
751801	SUSE Enterprise Linux Security Update for nodejs14 (SUSE-SU-2022:0715-1)	Vulnerability - level 5	Vuln
751810	OpenSUSE Security Update for expat (openSUSE-SU-2022:0713-1)	Vulnerability - level 5	Vuln
751820	OpenSUSE Security Update for nodejs14 (openSUSE-SU-2022:0715-1)	Vulnerability - level 5	Vuln
751824	OpenSUSE Security Update for nodejs8 (openSUSE-SU-2022:0704-1)	Vulnerability - level 5	Vuln
751826	OpenSUSE Security Update for nodejs8 (openSUSE-SU-22022:20000-2)	Vulnerability - level 5	Vuln
751831	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0768-1)	Vulnerability - level 3	Vuln
751832	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0765-1)	Vulnerability - level 3	Vuln
751833	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0757-1)	Vulnerability - level 3	Vuln
751835	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0767-1)	Vulnerability - level 3	Vuln
751836	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0759-1)	Vulnerability - level 4	Vuln
751837	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0762-1)	Vulnerability - level 4	Vuln
751838	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0766-1)	Vulnerability - level 3	Vuln
751851	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0768-1)	Vulnerability - level 3	Vuln
751852	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0755-1)	Vulnerability - level 3	Vuln
751853	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0760-1)	Vulnerability - level 3	Vuln
751855	SUSE Enterprise Linux Security Update for python-libxml2-python (SUSE-SU-2022:0802-1)	Vulnerability - level 4	Vuln
751859	OpenSUSE Security Update for python-libxml2-python (openSUSE-SU-2022:0802-1)	Vulnerability - level 4	Vuln
751909	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0928-1)	Vulnerability - level 5	Vuln
751911	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:0908-1)	Vulnerability - level 4	Vuln
751912	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0918-1)	Vulnerability - level 5	Vuln
751918	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0929-1)	Vulnerability - level 5	Vuln
751919	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:0931-1)	Vulnerability - level 3	Vuln
751921	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:0939-1)	Vulnerability - level 3	Vuln
751922	OpenSUSE Security Update for xen (openSUSE-SU-2022:0940-1)	Vulnerability - level 3	Vuln
751923	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:0946-1)	Vulnerability - level 3	Vuln
751925	OpenSUSE Security Update for bind (openSUSE-SU-2022:0945-1)	Vulnerability - level 3	Vuln
751927	OpenSUSE Security Update for bind (openSUSE-SU-2022:0946-1)	Vulnerability - level 3	Vuln
751935	SUSE Enterprise Linux Security Update for Open Virtual Private Network (OpenVPN) (SUSE-SU-2022:1029-1)	Vulnerability - level 5	Vuln
751936	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:1031-1)	Vulnerability - level 5	Vuln
751938	SUSE Enterprise Linux Security Update for Open Virtual Private Network (OpenVPN) (SUSE-SU-2022:1024-1)	Vulnerability - level 5	Vuln

751941	OpenSUSE Security Update for Open Virtual Private Network (OpenVPN) (openSUSE-SU-2022:1029-1)	Vulnerability - level 5	Vuln
751942	OpenSUSE Security Update for apache2 (openSUSE-SU-2022:1031-1)	Vulnerability - level 5	Vuln
751952	OpenSUSE Security Update for Linux Kernel (openSUSE-SU-2022:1039-1)	Vulnerability - level 4	Vuln
751956	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:1037-1)	Vulnerability - level 4	Vuln
751980	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:0151-1)	Vulnerability - level 3	Vuln
751997	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:0945-1)	Vulnerability - level 4	Vuln
751999	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0760-1)	Vulnerability - level 4	Vuln
752004	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:0940-1)	Vulnerability - level 3	Vuln
752016	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1039-1)	Vulnerability - level 4	Vuln
752030	SUSE Enterprise Linux Security Update for go1.17 (SUSE-SU-2022:1167-1)	Vulnerability - level 4	Vuln
752032	SUSE Enterprise Linux Security Update for go1.16 (SUSE-SU-2022:1164-1)	Vulnerability - level 4	Vuln
752036	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1183-1)	Vulnerability - level 4	Vuln
752039	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1196-1)	Vulnerability - level 5	Vuln
752042	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1197-1)	Vulnerability - level 4	Vuln
752048	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1266-1)	Vulnerability - level 5	Vuln
752052	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1255-1)	Vulnerability - level 5	Vuln
752053	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1267-1)	Vulnerability - level 5	Vuln
752054	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:1285-1)	Vulnerability - level 4	Vuln
752056	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1270-1)	Vulnerability - level 4	Vuln
752058	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1256-1)	Vulnerability - level 5	Vuln
752065	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:1300-1)	Vulnerability - level 4	Vuln
752068	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:1308-1)	Vulnerability - level 4	Vuln
752073	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:1359-1)	Vulnerability - level 4	Vuln
752075	SUSE Enterprise Linux Security Update for xen (SUSE-SU-2022:1408-1)	Vulnerability - level 4	Vuln
752120	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1651-1)	Vulnerability - level 4	Vuln
752122	SUSE Enterprise Linux Security Update for e2fsprogs (SUSE-SU-2022:1652-1)	Vulnerability - level 4	Vuln
752125	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1686-1)	Vulnerability - level 4	Vuln
752126	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1687-1)	Vulnerability - level 4	Vuln
752128	SUSE Enterprise Linux Security Update for e2fsprogs (SUSE-SU-2022:1688-1)	Vulnerability - level 4	Vuln

752139	SUSE Enterprise Linux Security Update for e2fsprogs (SUSE-SU-2022:1695-1)	Vulnerability - level 4	Vuln
752141	SUSE Enterprise Linux Security Update for e2fsprogs (SUSE-SU-2022:1718-1)	Vulnerability - level 4	Vuln
752142	SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2022:1717-1)	Vulnerability - level 5	Vuln
752156	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:1750-1)	Vulnerability - level 4	Vuln
752179	SUSE Enterprise Linux Security Update for wpa_supplicant (SUSE-SU-2022:1853-1)	Vulnerability - level 5	Vuln
752191	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:1616-1)	Vulnerability - level 4	Vuln
752208	SUSE Enterprise Linux Security Update for Open Virtual Private Network (OpenVPN) (SUSE-SU-2022:1934-1)	Vulnerability - level 5	Vuln
752228	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2078-1)	Vulnerability - level 4	Vuln
752230	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2022:2075-1)	Vulnerability - level 5	Vuln
752231	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2082-1)	Vulnerability - level 5	Vuln
752234	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2080-1)	Vulnerability - level 4	Vuln
752236	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1)(SUSE-SU-2022:2068-1)	Vulnerability - level 5	Vuln
752237	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2083-1)	Vulnerability - level 4	Vuln
752240	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2103-1)	Vulnerability - level 4	Vuln
752241	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (SUSE-SU-2022:2106-1)	Vulnerability - level 5	Vuln
752242	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2104-1)	Vulnerability - level 4	Vuln
752247	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:2101-1)	Vulnerability - level 5	Vuln
752248	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:2099-1)	Vulnerability - level 5	Vuln
752249	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2022:2098-1)	Vulnerability - level 5	Vuln
752250	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2111-1)	Vulnerability - level 4	Vuln
752251	SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2022:2134-1)	Vulnerability - level 5	Vuln
752254	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2116-1)	Vulnerability - level 4	Vuln
752266	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2022:2181-1)	Vulnerability - level 4	Vuln
752269	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2022:2180-1)	Vulnerability - level 4	Vuln
752272	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2022:2179-1)	Vulnerability - level 4	Vuln
752273	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2022:2182-1)	Vulnerability - level 5	Vuln
752276	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2173-1)	Vulnerability - level 3	Vuln
752280	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (SUSE-SU-2022:2197-1)	Vulnerability - level 5	Vuln
752283	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2022:2251-1)	Vulnerability - level 5	Vuln

752298	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2022:2308-1)	Vulnerability - level 5	Vuln
752301	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (SUSE-SU-2022:2309-1)	Vulnerability - level 5	Vuln
752302	SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:2294-1)	Vulnerability - level 5	Vuln
752305	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2022:2311-1)	Vulnerability - level 4	Vuln
752307	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:2302-1)	Vulnerability - level 5	Vuln
752308	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-3) (SUSE-SU-2022:2306-1)	Vulnerability - level 5	Vuln
752310	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2022:2312-1)	Vulnerability - level 4	Vuln
752323	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_0_0) (SUSE-SU-2022:2321-1)	Vulnerability - level 5	Vuln
752325	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-1_1) (SUSE-SU-2022:2328-1)	Vulnerability - level 4	Vuln
752326	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:2338-1)	Vulnerability - level 5	Vuln
752331	SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:2342-1)	Vulnerability - level 5	Vuln
752354	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2393-1)	Vulnerability - level 4	Vuln
752362	SUSE Enterprise Linux Security Update for nodejs14 (SUSE-SU-2022:2425-1)	Vulnerability - level 4	Vuln
752367	SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2022:2430-1)	Vulnerability - level 4	Vuln
752370	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2520-1)	Vulnerability - level 4	Vuln
752389	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:2552-1)	Vulnerability - level 4	Vuln
752457	SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:2713-1)	Vulnerability - level 4	Vuln
752490	SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2022:2855-1)	Vulnerability - level 5	Vuln
752529	SUSE Enterprise Linux Security Update for postgresql12 (SUSE-SU-2022:2958-1)	Vulnerability - level 4	Vuln
752584	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3265-1)	Vulnerability - level 4	Vuln
752589	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3264-1)	Vulnerability - level 4	Vuln
752591	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3274-1)	Vulnerability - level 4	Vuln
752592	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3282-1)	Vulnerability - level 4	Vuln
752594	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3293-1)	Vulnerability - level 4	Vuln
752596	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3291-1)	Vulnerability - level 4	Vuln
752615	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3408-1)	Vulnerability - level 5	Vuln
752632	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3450-1)	Vulnerability - level 5	Vuln
752702	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3693-1)	Vulnerability - level 4	Vuln
752708	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3704-1)	Vulnerability - level 4	Vuln

752750	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3844-1)	Vulnerability - level 4	Vuln
752794	SUSE Enterprise Linux Security Update for busybox (SUSE-SU-2022:3959-1)	Vulnerability - level 5	Vuln
752903	SUSE Enterprise Linux Security Update for busybox (SUSE-SU-2022:4253-1)	Vulnerability - level 5	Vuln
752995	SUSE Enterprise Linux Security Update for grafana (SUSE-SU-2022:4428-1)	Vulnerability - level 5	Vuln
753063	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)	Vulnerability - level 5	Vuln
753086	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0755-1)	Vulnerability - level 4	Vuln
753091	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2172-1)	Vulnerability - level 4	Vuln
753094	SUSE Enterprise Linux Security Update for go1.18 (SUSE-SU-2022:1410-1)	Vulnerability - level 4	Vuln
753148	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2615-1)	Vulnerability - level 4	Vuln
753151	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15) (SUSE-SU-2022:2709-1)	Vulnerability - level 4	Vuln
753157	SUSE Enterprise Linux Security Update for nodejs16 (SUSE-SU-2022:2491-1)	Vulnerability - level 4	Vuln
753167	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3288-1)	Vulnerability - level 4	Vuln
753176	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1676-1)	Vulnerability - level 4	Vuln
753184	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 11 for SLE 15 SP3) (SUSE-SU-2022:2738-1)	Vulnerability - level 4	Vuln
753216	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 16 for SLE 15 SP3) (SUSE-SU-2022:2727-1)	Vulnerability - level 4	Vuln
753219	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 14 for SLE 15 SP3) (SUSE-SU-2022:2726-1)	Vulnerability - level 4	Vuln
753236	SUSE Enterprise Linux Security Update for go1.17 (SUSE-SU-2022:1411-1)	Vulnerability - level 4	Vuln
753246	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15 SP1) (SUSE-SU-2022:2728-1)	Vulnerability - level 4	Vuln
753277	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 28 for SLE 15 SP1) (SUSE-SU-2022:2700-1)	Vulnerability - level 4	Vuln
753279	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0764-1)	Vulnerability - level 3	Vuln
753284	SUSE Enterprise Linux Security Update for containerd, docker (SUSE-SU-2022:0334-1)	Vulnerability - level 4	Vuln
753296	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2177-1)	Vulnerability - level 4	Vuln
753299	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1669-1)	Vulnerability - level 4	Vuln
753319	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 7 for SLE 15 SP3) (SUSE-SU-2022:2766-1)	Vulnerability - level 4	Vuln
753346	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 21 for SLE 15 SP2) (SUSE-SU-2022:2783-1)	Vulnerability - level 4	Vuln
753348	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1038-1)	Vulnerability - level 4	Vuln
753363	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 30 for SLE 15 SP1) (SUSE-SU-2022:2461-1)	Vulnerability - level 4	Vuln
753368	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2079-1)	Vulnerability - level 4	Vuln
753370	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3609-1)	Vulnerability - level 4	Vuln

753373	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1257-1)	Vulnerability - level 4	Vuln
753374	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3809-1)	Vulnerability - level 4	Vuln
753417	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1163-1)	Vulnerability - level 4	Vuln
753420	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15) (SUSE-SU-2022:2482-1)	Vulnerability - level 4	Vuln
753422	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1037-1)	Vulnerability - level 4	Vuln
753427	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1407-1)	Vulnerability - level 4	Vuln
753437	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0763-1)	Vulnerability - level 3	Vuln
753443	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15 SP2) (SUSE-SU-2022:2776-1)	Vulnerability - level 4	Vuln
753475	SUSE Enterprise Linux Security Update for nodejs16 (SUSE-SU-2022:2551-1)	Vulnerability - level 4	Vuln
753481	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 9 for SLE 15 SP3) (SUSE-SU-2022:2770-1)	Vulnerability - level 4	Vuln
753491	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP4) (SUSE-SU-2022:2854-1)	Vulnerability - level 4	Vuln
753532	OpenSUSE Security Update for apptainer (openSUSE-SU-2023:0018-1)	Vulnerability - level 5	Vuln
753631	SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:0305-1)	Vulnerability - level 4	Vuln
753634	SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:0306-1)	Vulnerability - level 4	Vuln
753636	SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:0310-1)	Vulnerability - level 4	Vuln
753637	SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:0308-1)	Vulnerability - level 4	Vuln
753640	SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2023:0312-1)	Vulnerability - level 4	Vuln
753647	SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:0311-1)	Vulnerability - level 4	Vuln
753649	SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:0309-1)	Vulnerability - level 4	Vuln
753698	SUSE Enterprise Linux Security Update for nodejs18 (SUSE-SU-2023:0419-1)	Vulnerability - level 5	Vuln
753736	SUSE Enterprise Linux Security Update for nrpe (SUSE-SU-2023:0586-1)	Vulnerability - level 2	Vuln
753795	SUSE Enterprise Linux Security Update for compat-openssl098 (SUSE-SU-2023:0581-1)	Vulnerability - level 3	Vuln
753852	SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:1684-1)	Vulnerability - level 4	Vuln
753866	SUSE Enterprise Linux Security Update for ldb, samba (SUSE-SU-2023:1687-1)	Vulnerability - level 3	Vuln
753868	SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:1683-1)	Vulnerability - level 4	Vuln
753869	SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:1682-1)	Vulnerability - level 4	Vuln
753947	SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2023:2048-1)	Vulnerability - level 3	Vuln
754047	SUSE Enterprise Linux Security Update for go1.18-openssl (SUSE-SU-2023:2312-1)	Vulnerability - level 4	Vuln
754072	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_0_0 (SUSE-SU-2023:0305-2)	Vulnerability - level 4	Vuln

754127	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_0_0 (SUSE-SU-2023:2624-1)	Vulnerability - level 3	Vuln
754128	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_1 (SUSE-SU-2023:2623-1)	Vulnerability - level 3	Vuln
754129	SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1_1 (SUSE-SU-2023:2622-1)	Vulnerability - level 3	Vuln
770043	Red Hat OpenShift Container Platform 4.6.9 Packages and Security Update (RHSA-2020:5615)	Vulnerability - level 4	Vuln
770136	Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2022:0557)	Vulnerability - level 3	Vuln
770138	Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:0055)	Vulnerability - level 4	Vuln
770140	Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:0927)	Vulnerability - level 4	Vuln
770160	Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:5729)	Vulnerability - level 4	Vuln
770161	Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:5068)	Vulnerability - level 5	Vuln
770162	Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:6094)	Vulnerability - level 5	Vuln
86018	IBM WebSphere Application Server Java SDK Multiple Vulnerabilities (April 2015 CPU)	Vulnerability - level 3	Practice
86171	HP System Management Homepage Multiple Vulnerabilities (HPSBMU03380)	Vulnerability - level 4	Practice
86343	HP System Management Homepage Multiple Vulnerabilities (HPSBMU03422)	Potential Vulnerability - level 3	Practice
86437	Apache Tomcat Multiple Vulnerabilities	Potential Vulnerability - level 3	Practice
86487	HP System Management Homepage Multiple Vulnerabilities (HPSBMU03546)	Vulnerability - level 5	Vuln
86493	Apache HTTP Server Client Certificate Authentication Bypass Vulnerability	Potential Vulnerability - level 3	Practice
86500	HPE System Management Homepage Multiple Vulnerabilities (HPSBMU03653)	Vulnerability - level 3	Vuln
86713	Apache CGI Byterange Request Denial of Service Vulnerability	Vulnerability - level 3	Practice
86724	Apache Tomcat Simultaneous Directory Listing Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
86766	BEA WebLogic Multiple Vulnerabilities (2007)	Potential Vulnerability - level 3	Practice
86777	Apache Tomcat Accept-Language Cross-Site Scripting Vulnerability	Potential Vulnerability - level 3	Practice
86779	Apache Tomcat SingleSignOn Remote Information Disclosure Vulnerability	Potential Vulnerability - level 3	Practice
86782	Apache Tomcat Multiple Cross-Site Scripting Vulnerabilities in Manager and Host Manager Web Applications	Potential Vulnerability - level 3	Practice
86784	Apache Tomcat 4 Sendmail Servlet of "Examples" Web Application Cross-Site Scripting Vulnerability	Vulnerability - level 3	Vuln
86787	Apache Tomcat 5 Cross-Site Scripting in implicit-objects.jsp of "Examples" Application	Vulnerability - level 3	Vuln
86788	Apache 2.x Multiple Vulnerabilities	Potential Vulnerability - level 3	Practice
86792	Apache Tomcat 6 Information Disclosure Vulnerability	Potential Vulnerability - level 3	Practice
86795	Apache Tomcat Juli Logging Component Elevated Privileges Vulnerability	Potential Vulnerability - level 2	Practice
86797	Apache Tomcat 5 and 6 Vulnerability in Native APR Connector	Potential Vulnerability - level 2	Practice
86799	Apache Tomcat 4 and 5 Default Cipher Configuration Information Disclosure Vulnerability	Potential Vulnerability - level 2	Practice

86801	Apache mod_ssl Certificate Revocation List Off-By-One Buffer Overflow Vulnerability	Vulnerability - level 3	Practice
86812	Apache 2.0 HTTP Server PCRE Integer Overflow Vulnerability	Vulnerability - level 3	Practice
86813	Apache 2.2 HTTP Server mod_proxy_balancer Multiple Vulnerabilities	Vulnerability - level 3	Practice
86818	Apache HTTP Server mod_proxy_ftp Wildcard Characters Cross-Site Scripting	Vulnerability - level 3	Vuln
86823	Apache Tomcat "RemoteFilterValve" Security Bypass Vulnerability	Potential Vulnerability - level 4	Practice
86842	Apache Tomcat Java AJP Connector Invalid Header Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
86846	HP System Management Homepage Code Execution and Denial of Service	Potential Vulnerability - level 4	Practice
86865	Apache Tomcat Directory Traversal Weaknesses and Security Issue	Potential Vulnerability - level 3	Practice
86879	Apache Tomcat Authentication Header Information Disclosure Vulnerability	Potential Vulnerability - level 2	Practice
86886	IBM HTTP Server Multiple Vulnerabilities (PM10658)	Potential Vulnerability - level 3	Practice
86901	Apache httpd "mod_proxy_http" Timeout Handling Information Disclosure Vulnerability	Potential Vulnerability - level 3	Practice
86905	Apache Tomcat 5.5.29 Transfer-Encoding Information Disclosure Vulnerability	Potential Vulnerability - level 2	Practice
86908	Apache HTTP Server mod_cache and mod_dav Undisclosed DoS Vulnerability	Potential Vulnerability - level 3	Practice
86935	Apache Tomcat "@ServletSecurity" Annotation Security Bypass Vulnerability	Potential Vulnerability - level 3	Practice
86937	Apache Tomcat 7.x Prior to 7.0.12 Multiple Vulnerabilities	Potential Vulnerability - level 3	Practice
86939	Apache Tomcat SecurityManager Security Bypass Vulnerability	Potential Vulnerability - level 3	Practice
86943	Apache Tomcat "@ServletSecurity" Annotation Security Bypass Vulnerability	Potential Vulnerability - level 2	Practice
87104	Apache Tomcat NIO Connector Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
87122	HP System Management Homepage Multiple Vulnerabilities (HPSBMU02786)	Potential Vulnerability - level 3	Practice
87123	HP System Management Homepage Multiple Vulnerabilities (HPSBMU02764)	Potential Vulnerability - level 3	Practice
87128	Apache Tomcat Denial of Service Vulnerabilities	Potential Vulnerability - level 3	Practice
87129	Apache Tomcat Security Constraints Bypass	Potential Vulnerability - level 3	Practice
87130	Apache Tomcat CSRF Prevention Filter Bypass	Potential Vulnerability - level 3	Practice
87156	Apache Prior to 2.4.4 and 2.2.24 Multiple Vulnerabilities	Potential Vulnerability - level 3	Practice
87183	WebSphere Application Server Java Multiple Vulnerabilities (Oracle CPU Feb 2013)	Vulnerability - level 3	Practice
87184	Apache HTTP Server 2.0.x mod_cache and mod_dav Undisclosed Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
87209	Apache Tomcat FormAuthenticator Session Hijacking Weakness	Potential Vulnerability - level 3	Practice
87210	Apache Tomcat Chunked Transfer Encoding Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
87229	IBM Websphere Application Server Ant Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
87233	Apache HTTP Server Prior to 2.2.25 Multiple Vulnerabilities	Potential Vulnerability - level 3	Practice

87245	Apache Tomcat Information Disclosure and Denial of Service Vulnerability	Potential Vulnerability - level 3	Practice
87246	Apache Tomcat Session Fixation Vulnerability	Vulnerability - level 3	Vuln
87263	Apache Tomcat Multiple Vulnerabilities	Potential Vulnerability - level 3	Practice
87265	Apache Tomcat Arbitrary File Upload Vulnerability	Vulnerability - level 4	Practice
87272	Apache Tomcat Input Validation Security Bypass Vulnerability	Potential Vulnerability - level 3	Practice
87273	IBM WebSphere Application Server 8.0 Fix Pack 10 Missing	Vulnerability - level 4	Vuln
87288	Oracle WebLogic Server Multiple Vulnerabilities (CPUAPR2017)	Vulnerability - level 5	Practice
87296	Apache HTTP Server Prior to 2.4.25 Multiple Vulnerabilities	Potential Vulnerability - level 4	Practice
87308	Apache Tomcat Multiple Vulnerabilities	Potential Vulnerability - level 3	Practice
87333	Oracle WebLogic Server Multiple Vulnerabilities (CPUAPR2018)	Vulnerability - level 5	Vuln
87335	IBM HTTP Server Multiple Vulnerabilities (swg22015347)	Vulnerability - level 5	Vuln
87344	Apache Tomcat Multiple Security Vulnerabilities	Potential Vulnerability - level 4	Practice
87396	Oracle WebLogic Server Multiple Vulnerabilities (CPUOCT2019)	Vulnerability - level 4	Practice
87399	Oracle WebLogic Server Samples Multiple Vulnerabilities (CPUOCT2019)	Vulnerability - level 3	Vuln
87451	IBM HTTP Server Multiple Vulnerabilities (6464029)	Vulnerability - level 3	Vuln
87458	Oracle WebLogic Server Multiple Vulnerabilities (CPUJUL2021)	Vulnerability - level 4	Practice
87486	IBM Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (6559296)	Vulnerability - level 4	Practice
87487	IBM Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (6560814)	Vulnerability - level 4	Vuln
900005	CBL-Mariner Linux Security Update for moby-buildx 0.4.1 (DEPRECATED)	Vulnerability - level 5	Vuln
900029	CBL-Mariner Linux Security Update for bind 9.16.3 (DEPRECATED)	Vulnerability - level 3	Vuln
900030	CBL-Mariner Linux Security Update for httpd 2.4.46 (DEPRECATED)	Vulnerability - level 4	Vuln
900036	CBL-Mariner Linux Security Update for unzip 6.0 (DEPRECATED)	Vulnerability - level 5	Vuln
900040	CBL-Mariner Linux Security Update for kernel 5.4.91 (DEPRECATED)	Vulnerability - level 4	Vuln
900044	CBL-Mariner Linux Security Update for libxml2 2.9.10 (DEPRECATED)	Vulnerability - level 4	Vuln
900045	CBL-Mariner Linux Security Update for postgresql 12.6 (DEPRECATED)	Vulnerability - level 3	Vuln
900055	CBL-Mariner Linux Security Update for grub2 2.06~rc1 (DEPRECATED)	Vulnerability - level 4	Vuln
900056	CBL-Mariner Linux Security Update for grub2 2.06~rc1 (DEPRECATED)	Vulnerability - level 2	Vuln
900065	CBL-Mariner Linux Security Update for bind 9.16.3 (DEPRECATED)	Vulnerability - level 3	Vuln
900068	CBL-Mariner Linux Security Update for dnsmasq 2.79 (DEPRECATED)	Vulnerability - level 4	Vuln
900109	CBL-Mariner Linux Security Update for openldap 2.4.50 (DEPRECATED)	Vulnerability - level 3	Vuln
900120	CBL-Mariner Linux Security Update for nghttp2 1.33.0 (DEPRECATED)	Vulnerability - level 3	Vuln
900125	CBL-Mariner Linux Security Update for libxml2 2.9.10 (DEPRECATED)	Vulnerability - level 3	Vuln
900145	CBL-Mariner Linux Security Update for openldap 2.4.50 (DEPRECATED)	Vulnerability - level 3	Vuln
900147	CBL-Mariner Linux Security Update for openvswitch 2.12.0 (DEPRECATED)	Vulnerability - level 4	Vuln
900155	CBL-Mariner Linux Security Update for curl 7.68.0 (DEPRECATED)	Vulnerability - level 3	Vuln
900168	CBL-Mariner Linux Security Update for kernel 5.4.72 (DEPRECATED)	Vulnerability - level 4	Vuln
900175	CBL-Mariner Linux Security Update for grub2 2.02 (DEPRECATED)	Vulnerability - level 3	Vuln

900176	CBL-Mariner Linux Security Update for util-linux 2.32.1 (DEPRECATED)	Vulnerability - level 4	Vuln
900182	CBL-Mariner Linux Security Update for mysql 8.0.22 (DEPRECATED)	Vulnerability - level 4	Vuln
900208	CBL-Mariner Linux Security Update for grub2 2.02 (DEPRECATED)	Vulnerability - level 2	Vuln
900310	CBL-Mariner Linux Security Update for go lang 1.15.13 (DEPRECATED)	Vulnerability - level 2	Vuln
900315	CBL-Mariner Linux Security Update for nodejs 14.17.2 (DEPRECATED)	Vulnerability - level 4	Vuln
900332	Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (5917)	Vulnerability - level 5	Vuln
900333	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (6005)	Vulnerability - level 5	Vuln
900363	Common Base Linux Mariner (CBL-Mariner) Security Update for moby-containerd (6154)	Vulnerability - level 4	Vuln
900386	Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (5487)	Vulnerability - level 4	Vuln
900406	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (6006)	Vulnerability - level 4	Vuln
900408	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6187)	Vulnerability - level 4	Vuln
900409	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6188)	Vulnerability - level 4	Vuln
900410	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6189)	Vulnerability - level 4	Vuln
900411	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6190)	Vulnerability - level 4	Vuln
900412	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6191)	Vulnerability - level 4	Vuln
900413	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6192)	Vulnerability - level 4	Vuln
900414	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6193)	Vulnerability - level 4	Vuln
900415	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6194)	Vulnerability - level 4	Vuln
900448	Common Base Linux Mariner (CBL-Mariner) Security Update for go lang (6176)	Vulnerability - level 3	Vuln
900449	Common Base Linux Mariner (CBL-Mariner) Security Update for go lang (6177)	Vulnerability - level 3	Vuln
900452	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6186)	Vulnerability - level 3	Vuln
900508	Common Base Linux Mariner (CBL-Mariner) Security Update for go lang (7115)	Vulnerability - level 4	Vuln
900510	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7129)	Vulnerability - level 5	Vuln
900511	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7130)	Vulnerability - level 5	Vuln
900512	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7131)	Vulnerability - level 5	Vuln
900513	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7132)	Vulnerability - level 4	Vuln
900514	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7133)	Vulnerability - level 4	Vuln
900515	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7134)	Vulnerability - level 4	Vuln
900613	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7831)	Vulnerability - level 5	Vuln
900618	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (8328)	Vulnerability - level 5	Vuln

900646	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (8471)	Vulnerability - level 3	Vuln
900675	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (8601)	Vulnerability - level 5	Vuln
900690	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (8630)	Vulnerability - level 4	Vuln
900697	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (8629)	Vulnerability - level 3	Vuln
900725	Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (8851)	Vulnerability - level 4	Vuln
900730	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8876)	Vulnerability - level 4	Vuln
900738	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8918) (DEPRECATED)	Vulnerability - level 4	Vuln
900755	Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (9006)	Vulnerability - level 5	Vuln
900757	Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (9008)	Vulnerability - level 5	Vuln
900774	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (9108)	Vulnerability - level 4	Vuln
900776	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (9109)	Vulnerability - level 3	Vuln
900801	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9283) (DEPRECATED)	Vulnerability - level 4	Vuln
900861	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9535) (DEPRECATED)	Vulnerability - level 4	Vuln
900864	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9546) (DEPRECATED)	Vulnerability - level 4	Vuln
900893	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9295) (DEPRECATED)	Vulnerability - level 4	Vuln
900910	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (6779-1)	Vulnerability - level 5	Vuln
900958	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6345-1)	Vulnerability - level 4	Vuln
900964	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6344-1)	Vulnerability - level 3	Vuln
900992	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6352-1)	Vulnerability - level 4	Vuln
900996	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6349-1)	Vulnerability - level 4	Vuln
901008	Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (8862-1)	Vulnerability - level 4	Vuln
901013	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6457-1)	Vulnerability - level 3	Vuln
901019	Common Base Linux Mariner (CBL-Mariner) Security Update for unzip (6932-1)	Vulnerability - level 4	Vuln
901028	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (9119) (DEPRECATED)	Vulnerability - level 3	Vuln
901054	Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (6484-1)	Vulnerability - level 4	Vuln
901060	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7156-1)	Vulnerability - level 5	Vuln
901099	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (7125-1)	Vulnerability - level 4	Vuln
901120	Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (6486-1)	Vulnerability - level 5	Vuln
901204	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6463-1)	Vulnerability - level 3	Vuln

901227	Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (6477-1)	Vulnerability - level 5	Vuln
901248	Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (6745-1)	Vulnerability - level 4	Vuln
901252	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6350-1)	Vulnerability - level 4	Vuln
901266	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7161-1)	Vulnerability - level 4	Vuln
901283	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (8334-1)	Vulnerability - level 5	Vuln
901302	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (9654) (DEPRECATED)	Vulnerability - level 5	Vuln
901304	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9653) (DEPRECATED)	Vulnerability - level 4	Vuln
901329	Common Base Linux Mariner (CBL-Mariner) Security Update for go lang (9535-1)	Vulnerability - level 4	Vuln
901330	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8918-1)	Vulnerability - level 4	Vuln
901339	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9283-1)	Vulnerability - level 4	Vuln
901370	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7159-1)	Vulnerability - level 4	Vuln
901410	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6347-1)	Vulnerability - level 4	Vuln
901413	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6460-1)	Vulnerability - level 4	Vuln
901446	Common Base Linux Mariner (CBL-Mariner) Security Update for go lang (6451-1)	Vulnerability - level 4	Vuln
901505	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6466-1)	Vulnerability - level 4	Vuln
901532	Common Base Linux Mariner (CBL-Mariner) Security Update for moby-containerd (6681-1)	Vulnerability - level 4	Vuln
901542	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (9649) (DEPRECATED)	Vulnerability - level 5	Vuln
901558	Common Base Linux Mariner (CBL-Mariner) Security Update for go lang (9547) (DEPRECATED)	Vulnerability - level 4	Vuln
901563	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7157-1)	Vulnerability - level 5	Vuln
901586	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (8624-1)	Vulnerability - level 4	Vuln
901589	Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (9018-1)	Vulnerability - level 5	Vuln
901636	Common Base Linux Mariner (CBL-Mariner) Security Update for e2fsprogs (9407) (DEPRECATED)	Vulnerability - level 4	Vuln
901647	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (6327) (DEPRECATED)	Vulnerability - level 3	Vuln
901658	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (9118) (DEPRECATED)	Vulnerability - level 4	Vuln
901674	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8922-1)	Vulnerability - level 4	Vuln
901677	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6459-1)	Vulnerability - level 3	Vuln
901725	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (8623-1)	Vulnerability - level 3	Vuln
901747	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6465-1)	Vulnerability - level 3	Vuln
901767	Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (6742-1)	Vulnerability - level 5	Vuln

901778	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7160-1)	Vulnerability - level 4	Vuln
901781	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6464-1)	Vulnerability - level 4	Vuln
901789	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6351-1)	Vulnerability - level 4	Vuln
901792	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7835-1)	Vulnerability - level 5	Vuln
901797	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (8603-1)	Vulnerability - level 5	Vuln
901800	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6348-1)	Vulnerability - level 4	Vuln
901802	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9527) (DEPRECATED)	Vulnerability - level 4	Vuln
901805	Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (9016-1)	Vulnerability - level 5	Vuln
901813	Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7158-1)	Vulnerability - level 5	Vuln
901819	Common Base Linux Mariner (CBL-Mariner) Security Update for busybox (6346-1)	Vulnerability - level 4	Vuln
901826	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6456-1)	Vulnerability - level 3	Vuln
901842	Common Base Linux Mariner (CBL-Mariner) Security Update for lldpd (7284) (DEPRECATED)	Vulnerability - level 4	Vuln
901843	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (8472-1)	Vulnerability - level 3	Vuln
901879	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8898-1)	Vulnerability - level 4	Vuln
901882	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (6780-1)	Vulnerability - level 4	Vuln
901910	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9646) (DEPRECATED)	Vulnerability - level 4	Vuln
901919	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6458-1)	Vulnerability - level 3	Vuln
901929	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6461-1)	Vulnerability - level 4	Vuln
901941	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (6452-1)	Vulnerability - level 4	Vuln
902010	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9653-1)	Vulnerability - level 4	Vuln
902028	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (9654-1)	Vulnerability - level 5	Vuln
902092	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9646-1)	Vulnerability - level 4	Vuln
902129	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9295-1)	Vulnerability - level 4	Vuln
902132	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (9649-1)	Vulnerability - level 5	Vuln
902171	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9896) (DEPRECATED)	Vulnerability - level 2	Vuln
902175	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9910) (DEPRECATED)	Vulnerability - level 2	Vuln
902190	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9546-1)	Vulnerability - level 4	Vuln
902239	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (6327-1)	Vulnerability - level 3	Vuln
902274	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9547-1)	Vulnerability - level 4	Vuln

902283	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (9527-1)	Vulnerability - level 4	Vuln
902300	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (9118-1)	Vulnerability - level 4	Vuln
902324	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (9119-1)	Vulnerability - level 3	Vuln
902361	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (9971) (DEPRECATED)	Vulnerability - level 5	Vuln
902389	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (9967-1)	Vulnerability - level 5	Vuln
902391	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9910-1)	Vulnerability - level 2	Vuln
902455	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10126) (DEPRECATED)	Vulnerability - level 4	Vuln
902459	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10122) (DEPRECATED)	Vulnerability - level 4	Vuln
902472	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10113) (DEPRECATED)	Vulnerability - level 4	Vuln
902477	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (9971-1)	Vulnerability - level 5	Vuln
902480	Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10135) (DEPRECATED)	Vulnerability - level 4	Vuln
902523	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10138)	Vulnerability - level 3	Vuln
902528	Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (10152) (DEPRECATED)	Vulnerability - level 4	Vuln
902535	Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (10149) (DEPRECATED)	Vulnerability - level 4	Vuln
902554	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10109)	Vulnerability - level 4	Vuln
902602	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10406) (DEPRECATED)	Vulnerability - level 3	Vuln
902603	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10401)	Vulnerability - level 3	Vuln
902651	Common Base Linux Mariner (CBL-Mariner) Security Update for lldpd (10443) (DEPRECATED)	Vulnerability - level 4	Vuln
902704	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9896-1)	Vulnerability - level 2	Vuln
902706	Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (10152-1)	Vulnerability - level 4	Vuln
902809	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3496)	Vulnerability - level 4	Vuln
902815	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3945)	Vulnerability - level 4	Vuln
902823	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3931)	Vulnerability - level 4	Vuln
902832	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3946)	Vulnerability - level 4	Vuln
902840	Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (4235)	Vulnerability - level 4	Vuln
902859	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (4177)	Vulnerability - level 5	Vuln
902870	Common Base Linux Mariner (CBL-Mariner) Security Update for nghttp2 (1936)	Vulnerability - level 4	Vuln
902876	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3627)	Vulnerability - level 4	Vuln
902878	Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (4236)	Vulnerability - level 4	Vuln

902889	Common Base Linux Mariner (CBL-Mariner) Security Update for postgresql (4338)	Vulnerability - level 4	Vuln
902896	Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (3653)	Vulnerability - level 4	Vuln
902966	Common Base Linux Mariner (CBL-Mariner) Security Update for dnsmasq (3815)	Vulnerability - level 4	Vuln
902990	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3935)	Vulnerability - level 4	Vuln
902995	Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (4371)	Vulnerability - level 5	Vuln
902997	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (4170)	Vulnerability - level 4	Vuln
903005	Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (3830)	Vulnerability - level 4	Vuln
90303	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (MS06-012)	Vulnerability - level 5	Vuln
903053	Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (4411)	Vulnerability - level 4	Vuln
90307	Microsoft Outlook Express Cumulative Security Update Missing (MS06-016)	Vulnerability - level 4	Vuln
903083	Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (3831)	Vulnerability - level 4	Vuln
903098	Common Base Linux Mariner (CBL-Mariner) Security Update for unzip (2670)	Vulnerability - level 4	Vuln
903104	Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (5424)	Vulnerability - level 4	Vuln
903107	Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (1831)	Vulnerability - level 4	Vuln
903149	Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (1832)	Vulnerability - level 4	Vuln
903161	Common Base Linux Mariner (CBL-Mariner) Security Update for openvswitch (4019)	Vulnerability - level 4	Vuln
903172	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (3907)	Vulnerability - level 4	Vuln
903216	Common Base Linux Mariner (CBL-Mariner) Security Update for dnsmasq (3813)	Vulnerability - level 4	Vuln
903226	Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (3881)	Vulnerability - level 3	Vuln
903277	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (2558)	Vulnerability - level 3	Vuln
903289	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3934)	Vulnerability - level 3	Vuln
903304	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1825)	Vulnerability - level 3	Vuln
903311	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (5296)	Vulnerability - level 3	Vuln
90334	PC Tools AntiVirus Local Privilege Escalation Vulnerability	Vulnerability - level 3	Vuln
903389	Common Base Linux Mariner (CBL-Mariner) Security Update for dnsmasq (3789)	Vulnerability - level 3	Vuln
903453	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3933)	Vulnerability - level 3	Vuln
903455	Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (4195)	Vulnerability - level 3	Vuln
903456	Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (4408)	Vulnerability - level 4	Vuln
903462	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1822)	Vulnerability - level 3	Vuln
903483	Common Base Linux Mariner (CBL-Mariner) Security Update for curl (3675)	Vulnerability - level 2	Vuln

903497	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1827)	Vulnerability - level 3	Vuln
903518	Common Base Linux Mariner (CBL-Mariner) Security Update for bind (4176)	Vulnerability - level 3	Vuln
903552	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (2557)	Vulnerability - level 3	Vuln
903576	Common Base Linux Mariner (CBL-Mariner) Security Update for dnsmasq (3790)	Vulnerability - level 3	Vuln
903689	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1823)	Vulnerability - level 3	Vuln
903731	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10798)	Vulnerability - level 4	Vuln
903813	Common Base Linux Mariner (CBL-Mariner) Security Update for lldpd (10443-1)	Vulnerability - level 4	Vuln
903824	Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (10149-1)	Vulnerability - level 4	Vuln
903825	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10792)	Vulnerability - level 4	Vuln
903896	Common Base Linux Mariner (CBL-Mariner) Security Update for e2fsprogs (9407-1)	Vulnerability - level 4	Vuln
90391	Windows Kernel Could Allow Elevation of Privilege (MS07-022)	Vulnerability - level 3	Vuln
903995	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10406-1)	Vulnerability - level 3	Vuln
904002	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10135-1)	Vulnerability - level 3	Vuln
904096	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10798-1)	Vulnerability - level 4	Vuln
904114	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10792-1)	Vulnerability - level 4	Vuln
904154	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10138-1)	Vulnerability - level 3	Vuln
904159	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10401-1)	Vulnerability - level 3	Vuln
90438	Microsoft DirectX Remote Code Execution Vulnerabilities (MS08-033)	Vulnerability - level 4	Vuln
90443	Active Directory Denial of Service Vulnerability (MS08-035)	Vulnerability - level 3	Vuln
90449	Microsoft Windows Messenger Information Disclosure Vulnerability (MS08-050)	Vulnerability - level 4	Vuln
90452	Microsoft Visual Studio "Msmask32.ocx" ActiveX Control Remote Buffer Overflow Vulnerability (MS08-070)	Vulnerability - level 4	Vuln
90473	Microsoft Visual Basic Runtime Extended Files Remote Code Execution Vulnerability (MS08-070)	Vulnerability - level 4	Vuln
904808	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10122-1)	Vulnerability - level 3	Vuln
904817	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12311)	Vulnerability - level 5	Vuln
904821	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12318)	Vulnerability - level 5	Vuln
904823	Common Base Linux Mariner (CBL-Mariner) Security Update for dhcp (12321)	Vulnerability - level 5	Vuln
904834	Common Base Linux Mariner (CBL-Mariner) Security Update for nss (12397)	Vulnerability - level 5	Vuln
904838	Common Base Linux Mariner (CBL-Mariner) Security Update for nss (12398)	Vulnerability - level 5	Vuln
904844	Common Base Linux Mariner (CBL-Mariner) Security Update for libdb (12354)	Vulnerability - level 5	Vuln
904858	Common Base Linux Mariner (CBL-Mariner) Security Update for heimdal (12349)	Vulnerability - level 5	Vuln

904875	Common Base Linux Mariner (CBL-Mariner) Security Update for rust (12429)	Vulnerability - level 5	Vuln
904879	Common Base Linux Mariner (CBL-Mariner) Security Update for heimdal (12348)	Vulnerability - level 5	Vuln
904886	Common Base Linux Mariner (CBL-Mariner) Security Update for libdb (12353)	Vulnerability - level 5	Vuln
904913	Common Base Linux Mariner (CBL-Mariner) Security Update for fluent-bit (12330)	Vulnerability - level 5	Vuln
904927	Common Base Linux Mariner (CBL-Mariner) Security Update for perl-DBD-SQLite (12407)	Vulnerability - level 5	Vuln
904929	Common Base Linux Mariner (CBL-Mariner) Security Update for perl-DBD-SQLite (12409)	Vulnerability - level 5	Vuln
904940	Common Base Linux Mariner (CBL-Mariner) Security Update for python2 (12411)	Vulnerability - level 5	Vuln
904944	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12306)	Vulnerability - level 5	Vuln
904958	Common Base Linux Mariner (CBL-Mariner) Security Update for mozjs60 (12365)	Vulnerability - level 5	Vuln
904960	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (12303)	Vulnerability - level 5	Vuln
904962	Common Base Linux Mariner (CBL-Mariner) Security Update for mozjs60 (12372)	Vulnerability - level 5	Vuln
904966	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12317)	Vulnerability - level 5	Vuln
904967	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12319)	Vulnerability - level 5	Vuln
904969	Common Base Linux Mariner (CBL-Mariner) Security Update for mozjs60 (12366)	Vulnerability - level 5	Vuln
904986	Common Base Linux Mariner (CBL-Mariner) Security Update for libdb (12513)	Vulnerability - level 5	Vuln
904991	Common Base Linux Mariner (CBL-Mariner) Security Update for dhcp (12482)	Vulnerability - level 5	Vuln
905012	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12479)	Vulnerability - level 5	Vuln
905020	Common Base Linux Mariner (CBL-Mariner) Security Update for rust (12640)	Vulnerability - level 5	Vuln
90503	Microsoft DirectShow Remote Code Execution Vulnerability (MS09-028)	Vulnerability - level 4	Vuln
905040	Common Base Linux Mariner (CBL-Mariner) Security Update for nss (12598)	Vulnerability - level 5	Vuln
905054	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12469)	Vulnerability - level 5	Vuln
905065	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12465)	Vulnerability - level 5	Vuln
905073	Common Base Linux Mariner (CBL-Mariner) Security Update for nss (12597)	Vulnerability - level 5	Vuln
905078	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12478)	Vulnerability - level 5	Vuln
905086	Common Base Linux Mariner (CBL-Mariner) Security Update for libdb (12510)	Vulnerability - level 5	Vuln
905122	Common Base Linux Mariner (CBL-Mariner) Security Update for heimdal (12496)	Vulnerability - level 5	Vuln
905130	Common Base Linux Mariner (CBL-Mariner) Security Update for heimdal (12495)	Vulnerability - level 5	Vuln
905153	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12472)	Vulnerability - level 5	Vuln
905437	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13302)	Vulnerability - level 4	Vuln

905438	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13310)	Vulnerability - level 4	Vuln
905439	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13301)	Vulnerability - level 4	Vuln
905441	Common Base Linux Mariner (CBL-Mariner) Security Update for shim-unsigned-x64 (13315)	Vulnerability - level 4	Vuln
905442	Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13311)	Vulnerability - level 4	Vuln
905444	Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13313)	Vulnerability - level 4	Vuln
905445	Common Base Linux Mariner (CBL-Mariner) Security Update for shim-unsigned-aarch64 (13314)	Vulnerability - level 4	Vuln
905446	Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13312)	Vulnerability - level 4	Vuln
905447	Common Base Linux Mariner (CBL-Mariner) Security Update for shim-unsigned-x64 (13336)	Vulnerability - level 4	Vuln
905450	Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13332)	Vulnerability - level 4	Vuln
905454	Common Base Linux Mariner (CBL-Mariner) Security Update for shim-unsigned-aarch64 (13335)	Vulnerability - level 4	Vuln
905456	Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13334)	Vulnerability - level 4	Vuln
905457	Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13333)	Vulnerability - level 4	Vuln
905458	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13319)	Vulnerability - level 4	Vuln
905459	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13318)	Vulnerability - level 4	Vuln
905460	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13317)	Vulnerability - level 4	Vuln
905464	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13352)	Vulnerability - level 4	Vuln
905468	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13347)	Vulnerability - level 4	Vuln
905469	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13351)	Vulnerability - level 4	Vuln
905478	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13326-1)	Vulnerability - level 4	Vuln
905481	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13325-1)	Vulnerability - level 4	Vuln
905483	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13323-1)	Vulnerability - level 4	Vuln
905503	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13352-1)	Vulnerability - level 4	Vuln
905506	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13310-1)	Vulnerability - level 4	Vuln
905538	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13351-1)	Vulnerability - level 4	Vuln
905551	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13566)	Vulnerability - level 5	Vuln
905552	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13564)	Vulnerability - level 5	Vuln
905555	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13566-1)	Vulnerability - level 5	Vuln
905562	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (13564-1)	Vulnerability - level 5	Vuln
905627	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13698)	Vulnerability - level 4	Vuln

905629	Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13700)	Vulnerability - level 4	Vuln
905630	Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13705)	Vulnerability - level 4	Vuln
905632	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13701)	Vulnerability - level 4	Vuln
905634	Common Base Linux Mariner (CBL-Mariner) Security Update for reaper (13704)	Vulnerability - level 4	Vuln
90570	Microsoft Internet Explorer Cumulative Security Update (MS09-072 and KB977981)	Vulnerability - level 4	Vuln
905748	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3627-1)	Vulnerability - level 4	Vuln
90575	Microsoft Embedded OpenType Font Engine Remote Code Execution Vulnerability (MS10-001)	Vulnerability - level 5	Vuln
905793	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (2557-1)	Vulnerability - level 3	Vuln
905821	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3945-1)	Vulnerability - level 4	Vuln
905838	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10406-2)	Vulnerability - level 3	Vuln
905856	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9653-2)	Vulnerability - level 4	Vuln
905865	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9896-2)	Vulnerability - level 2	Vuln
905904	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3933-1)	Vulnerability - level 3	Vuln
905934	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3935-1)	Vulnerability - level 4	Vuln
905953	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1825-1)	Vulnerability - level 3	Vuln
905993	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10798-2)	Vulnerability - level 4	Vuln
906025	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10122-2)	Vulnerability - level 3	Vuln
906063	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (2558-1)	Vulnerability - level 3	Vuln
90608	Microsoft .NET Framework Tampering Vulnerability (MS10-041)	Vulnerability - level 4	Vuln
906084	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8918-2)	Vulnerability - level 4	Vuln
906098	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3946-1)	Vulnerability - level 4	Vuln
906110	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10135-2)	Vulnerability - level 3	Vuln
906127	Common Base Linux Mariner (CBL-Mariner) Security Update for unzip (2670-1)	Vulnerability - level 4	Vuln
906136	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (8471-1)	Vulnerability - level 3	Vuln
906145	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3931-1)	Vulnerability - level 4	Vuln
906151	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9283-2)	Vulnerability - level 4	Vuln
906187	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3496-1)	Vulnerability - level 4	Vuln
906208	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (1823-1)	Vulnerability - level 3	Vuln
906216	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (3934-1)	Vulnerability - level 3	Vuln
906270	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6461-2)	Vulnerability - level 4	Vuln

906278	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10792-2)	Vulnerability - level 4	Vuln
906281	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6459-2)	Vulnerability - level 3	Vuln
906309	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6460-2)	Vulnerability - level 4	Vuln
906321	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6465-2)	Vulnerability - level 3	Vuln
906325	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6456-2)	Vulnerability - level 3	Vuln
906368	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (10109-2)	Vulnerability - level 3	Vuln
906372	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9910-2)	Vulnerability - level 2	Vuln
906378	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8922-2)	Vulnerability - level 4	Vuln
906381	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6457-2)	Vulnerability - level 3	Vuln
906392	Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (8472-2)	Vulnerability - level 3	Vuln
906398	Common Base Linux Mariner (CBL-Mariner) Security Update for unzip (6932-2)	Vulnerability - level 4	Vuln
906457	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6464-2)	Vulnerability - level 4	Vuln
906461	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6466-2)	Vulnerability - level 4	Vuln
906465	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10401-2)	Vulnerability - level 3	Vuln
906478	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6463-2)	Vulnerability - level 3	Vuln
906505	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (6458-2)	Vulnerability - level 3	Vuln
906506	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10138-2)	Vulnerability - level 3	Vuln
906512	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9295-2)	Vulnerability - level 4	Vuln
906514	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9646-2)	Vulnerability - level 4	Vuln
906757	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13302-1)	Vulnerability - level 3	Vuln
906765	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13347-1)	Vulnerability - level 4	Vuln
906766	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13301-1)	Vulnerability - level 4	Vuln
906772	Common Base Linux Mariner (CBL-Mariner) Security Update for cloud-hypervisor (13701-1)	Vulnerability - level 4	Vuln
90803	Microsoft Combined Security Update for Microsoft Office, Windows, .NET Framework and Silverlight (MS12-034)	Vulnerability - level 5	Vuln
90817	Microsoft Data Access Components Remote Code Execution Vulnerability (MS12-045)	Vulnerability - level 5	Vuln
90852	Microsoft XML Core Services Remote Code Execution Vulnerability (MS13-002)	Vulnerability - level 4	Vuln
90894	Microsoft Windows Kernel-Mode Drivers Remote Code Execution (MS13-053)	Vulnerability - level 5	Vuln
90948	Microsoft Windows File Handling Component Remote Code Execution Vulnerability (MS14-019)	Vulnerability - level 4	Vuln
90964	Microsoft Windows DirectShow Privilege Escalation Vulnerability (MS14-041)	Vulnerability - level 4	Vuln
91108	Microsoft .Net Framework Multiple Vulnerabilities (MS15-118)	Vulnerability - level 3	Vuln

91128	Microsoft Windows 2003 .NET Framework Multiple Vulnerabilities (MS15-118) (Extended Support)	Vulnerability - level 3	Vuln
91168	Microsoft Edge Cumulative Security Update (MS16-011)	Vulnerability - level 4	Vuln
91201	Microsoft .NET Framework Remote Code Execution Vulnerability (MS16-041)	Vulnerability - level 4	Vuln
91355	Microsoft Windows Security Update April 2017	Vulnerability - level 5	Vuln
91356	Microsoft Silverlight 5 Security Update April 2017	Vulnerability - level 5	Vuln
91366	Microsoft Windows 2003 Graphics Component April 2017 (KB4014652, KB4014794, KB4015195, KB4015380, KB4015383) (Extended Support)	Vulnerability - level 4	Vuln
91369	Microsoft Windows Security Update May 2017	Vulnerability - level 4	Vuln
91374	Microsoft Windows 2003 SMB Information Disclosure Vulnerability May 2017 (KB4018466) (Extended Support)	Vulnerability - level 5	Vuln
91411	Microsoft Windows Security Update October 2017 (KRACK Attack) (ROCA)	Vulnerability - level 4	Vuln
91469	Microsoft Windows Intel Microcode Updates Not Installed	Vulnerability - level 4	Vuln
91499	Microsoft Azure Stack 1809 Multiple Security Vulnerabilities	Vulnerability - level 4	Vuln
91553	Microsoft Windows Security Update for July 2019	Vulnerability - level 5	Vuln
91555	Microsoft Azure Stack 1907 Multiple Security Vulnerabilities	Vulnerability - level 4	Vuln
91609	Microsoft Windows Security Update for March 2020	Vulnerability - level 5	Vuln
91671	Microsoft Windows Security Feature Bypass in GRUB (ADV200011) (BootHole)	Potential Vulnerability - level 4	Practice
91739	Microsoft Windows Security Update for February 2021	Vulnerability - level 4	Vuln
91762	Microsoft Windows Security Update for May 2021	Vulnerability - level 5	Vuln
91780	Microsoft Azure Stack Hub Security Updates - February 2021	Vulnerability - level 5	Vuln
91781	IBM Integration Bus and IBM App Connect Enterprise Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (6444817,6444819)	Potential Vulnerability - level 3	Practice
91782	IBM Integration Bus and IBM App Connect Enterprise Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (6463979)	Potential Vulnerability - level 3	Practice
91783	IBM Integration Bus and IBM App Connect Enterprise Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (6466315)	Potential Vulnerability - level 3	Practice
91784	IBM Integration Bus and IBM App Connect Enterprise Node.js Multiple Vulnerabilities (6467639)	Potential Vulnerability - level 3	Practice
91822	Microsoft Visual Studio Security Update for October 2021	Vulnerability - level 3	Vuln
91831	Microsoft Visual Studio Security Update - November 2021	Vulnerability - level 4	Vuln
940000	AlmaLinux Security Update for curl (ALSA-2021:1610)	Vulnerability - level 3	Vuln
940020	AlmaLinux Security Update for edk2 (ALSA-2021:4198)	Vulnerability - level 3	Vuln
940043	AlmaLinux Security Update for bind (ALSA-2021:1989)	Vulnerability - level 4	Vuln
940046	AlmaLinux Security Update for fwupd (ALSA-2021:2566)	Vulnerability - level 3	Vuln
940071	AlmaLinux Security Update for idm:DL1 and idm:client (ALSA-2020:4670)	Vulnerability - level 3	Vuln
940076	AlmaLinux Security Update for libxml2 (ALSA-2020:4479)	Vulnerability - level 3	Vuln
940088	AlmaLinux Security Update for mingw (ALSA-2021:1968)	Vulnerability - level 3	Vuln
940099	AlmaLinux Security Update for nodejs:10 (ALSA-2021:0735)	Vulnerability - level 4	Vuln
940104	AlmaLinux Security Update for nodejs:12 (ALSA-2020:2852)	Vulnerability - level 4	Vuln
940108	AlmaLinux Security Update for bind (ALSA-2021:4384)	Vulnerability - level 3	Vuln
940128	AlmaLinux Security Update for nodejs:12 (ALSA-2020:4272)	Vulnerability - level 3	Vuln
940150	AlmaLinux Security Update for subversion:1.10 (ALSA-2020:4712)	Vulnerability - level 3	Vuln
940174	AlmaLinux Security Update for kernel (ALSA-2021:4647)	Vulnerability - level 4	Vuln
940192	AlmaLinux Security Update for bind (ALSA-2021:0670)	Vulnerability - level 4	Vuln
940196	AlmaLinux Security Update for postgresql:9.6 (ALSA-2021:2360)	Vulnerability - level 4	Vuln
940199	AlmaLinux Security Update for nodejs:10 (ALSA-2020:2848)	Vulnerability - level 4	Vuln
940213	AlmaLinux Security Update for nodejs:14 (ALSA-2021:0744)	Vulnerability - level 4	Vuln
940216	AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2021:4156)	Vulnerability - level 3	Vuln
940217	AlmaLinux Security Update for nodejs:12 (ALSA-2021:3623)	Vulnerability - level 4	Vuln
940218	AlmaLinux Security Update for postgresql:13 (ALSA-2021:2375)	Vulnerability - level 4	Vuln

940231	AlmaLinux Security Update for nodejs:10 (ALSA-2021:0548)	Vulnerability - level 3	Vuln
940234	AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2021:4424)	Vulnerability - level 3	Vuln
940239	AlmaLinux Security Update for nghttp2 (ALSA-2020:2755)	Vulnerability - level 4	Vuln
940259	AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2020:5476)	Vulnerability - level 4	Vuln
940265	AlmaLinux Security Update for kernel (ALSA-2021:4356)	Vulnerability - level 3	Vuln
940266	AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2021:5226)	Vulnerability - level 3	Vuln
940294	AlmaLinux Security Update for microcode_ctl (ALSA-2021:2308)	Vulnerability - level 4	Vuln
940297	AlmaLinux Security Update for httpd:2.4 (ALSA-2021:3816)	Vulnerability - level 4	Vuln
940314	AlmaLinux Security Update for shim (ALSA-2021:1734)	Vulnerability - level 3	Vuln
940320	AlmaLinux Security Update for grub2 (ALSA-2021:0696)	Vulnerability - level 3	Vuln
940337	AlmaLinux Security Update for sqlite (ALSA-2020:4442)	Vulnerability - level 3	Vuln
940343	AlmaLinux Security Update for postgresql:10 (ALSA-2021:2361)	Vulnerability - level 4	Vuln
940348	AlmaLinux Security Update for pki-core:10.6 and pki-deps:10.6 (ALSA-2020:4847)	Vulnerability - level 3	Vuln
940369	AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2021:1024)	Vulnerability - level 4	Vuln
940375	AlmaLinux Security Update for libxml2 (ALSA-2021:2569)	Vulnerability - level 3	Vuln
940381	AlmaLinux Security Update for libvncserver (ALSA-2021:1811)	Vulnerability - level 3	Vuln
940386	AlmaLinux Security Update for sqlite (ALSA-2021:4396)	Vulnerability - level 3	Vuln
940388	AlmaLinux Security Update for nodejs:14 (ALSA-2021:3666)	Vulnerability - level 4	Vuln
940391	AlmaLinux Security Update for microcode_ctl (ALSA-2021:3027)	Vulnerability - level 4	Vuln
940396	AlmaLinux Security Update for dnsmasq (ALSA-2021:0150)	Vulnerability - level 4	Vuln
940408	AlmaLinux Security Update for kernel (ALSA-2021:0558)	Vulnerability - level 4	Vuln
940411	AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2021:5160)	Vulnerability - level 2	Vuln
940413	AlmaLinux Security Update for postgresql:12 (ALSA-2021:2372)	Vulnerability - level 4	Vuln
940414	AlmaLinux Security Update for libvncserver (ALSA-2020:3385)	Vulnerability - level 4	Vuln
940419	AlmaLinux Security Update for nodejs:12 (ALSA-2021:0734)	Vulnerability - level 4	Vuln
940428	AlmaLinux Security Update for grafana (ALSA-2022:0001)	Vulnerability - level 2	Vuln
940448	AlmaLinux Security Update for nodejs:14 (ALSA-2022:0350)	Vulnerability - level 5	Vuln
940460	AlmaLinux Security Update for firefox (ALSA-2022:0818)	Vulnerability - level 5	Vuln
940465	AlmaLinux Security Update for thunderbird (ALSA-2022:0845)	Vulnerability - level 5	Vuln
940468	AlmaLinux Security Update for libxml2 (ALSA-2022:0899)	Vulnerability - level 4	Vuln
940471	AlmaLinux Security Update for httpd:2.4 (ALSA-2022:0891)	Vulnerability - level 5	Vuln
940473	AlmaLinux Security Update for expat (ALSA-2022:0951)	Vulnerability - level 5	Vuln
940474	AlmaLinux Security Update for httpd:2.4 (ALSA-2022:1049)	Vulnerability - level 5	Vuln
940490	AlmaLinux Security Update for xmlrpc-c (ALSA-2022:1643)	Vulnerability - level 5	Vuln
940504	AlmaLinux Security Update for subversion:1.10 (ALSA-2019:2512)	Vulnerability - level 4	Vuln
940517	AlmaLinux Security Update for kernel (ALSA-2022:1988)	Vulnerability - level 5	Vuln
940527	AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2022:1819)	Vulnerability - level 5	Vuln
940543	AlmaLinux Security Update for bind (ALSA-2022:2092)	Vulnerability - level 3	Vuln
940561	AlmaLinux Security Update for python27:2.7 (ALSA-2019:0981)	Vulnerability - level 5	Vuln
940573	AlmaLinux Security Update for pki-deps:10.6 (ALSA-2019:1529)	Vulnerability - level 5	Vuln
940591	AlmaLinux Security Update for expat (ALSA-2022:5314)	Vulnerability - level 4	Vuln
940594	AlmaLinux Security Update for kernel-rt (ALSA-2022:5565)	Vulnerability - level 4	Vuln
940596	AlmaLinux Security Update for kernel (ALSA-2022:5564)	Vulnerability - level 4	Vuln
940611	AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2022:5818)	Vulnerability - level 5	Vuln
940618	AlmaLinux Security Update for kernel (ALSA-2022:5249)	Vulnerability - level 5	Vuln
940631	AlmaLinux Security Update for expat (ALSA-2022:5244)	Vulnerability - level 4	Vuln
940638	AlmaLinux Security Update for kernel-rt (ALSA-2022:5267)	Vulnerability - level 5	Vuln
940649	AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2022:6224)	Vulnerability - level 5	Vuln
940654	AlmaLinux Security Update for nodejs:14 (ALSA-2022:6448)	Vulnerability - level 5	Vuln
940678	AlmaLinux Security Update for nodejs and nodejs-nodemon (ALSA-2022:6595)	Vulnerability - level 5	Vuln
940709	AlmaLinux Security Update for kernel-rt (ALSA-2022:7134)	Vulnerability - level 4	Vuln

940719	AlmaLinux Security Update for kernel (ALSA-2022:7110)	Vulnerability - level 4	Vuln
940732	AlmaLinux Security Update for kernel (ALSA-2022:7683)	Vulnerability - level 4	Vuln
940734	AlmaLinux Security Update for bind (ALSA-2022:7790)	Vulnerability - level 4	Vuln
940735	AlmaLinux Security Update for e2fsprogs (ALSA-2022:7720)	Vulnerability - level 4	Vuln
940736	AlmaLinux Security Update for xmlrpc-c (ALSA-2022:7692)	Vulnerability - level 5	Vuln
940738	AlmaLinux Security Update for mingw-expat (ALSA-2022:7811)	Vulnerability - level 5	Vuln
940741	AlmaLinux Security Update for httpd:2.4 (ALSA-2022:7647)	Vulnerability - level 5	Vuln
940749	AlmaLinux Security Update for bind9.16 (ALSA-2022:7643)	Vulnerability - level 4	Vuln
940766	AlmaLinux Security Update for kernel-rt (ALSA-2022:7444)	Vulnerability - level 4	Vuln
940788	AlmaLinux Security Update for e2fsprogs (ALSA-2022:8361)	Vulnerability - level 4	Vuln
940793	AlmaLinux Security Update for dhcp (ALSA-2022:8385)	Vulnerability - level 4	Vuln
940798	AlmaLinux Security Update for kernel (ALSA-2022:8267)	Vulnerability - level 4	Vuln
940822	AlmaLinux Security Update for bind (ALSA-2022:8068)	Vulnerability - level 4	Vuln
940823	AlmaLinux Security Update for httpd (ALSA-2022:8067)	Vulnerability - level 5	Vuln
940843	AlmaLinux Security Update for kernel-rt (ALSA-2022:7933)	Vulnerability - level 4	Vuln
940941	AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:0946)	Vulnerability - level 4	Vuln
940962	AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:1405)	Vulnerability - level 4	Vuln
941044	AlmaLinux Security Update for edk2 (ALSA-2023:2165)	Vulnerability - level 5	Vuln
941103	AlmaLinux Security Update for edk2 (ALSA-2023:2932)	Vulnerability - level 4	Vuln
960001	Rocky Linux Security Update for microcode_ctl (RLSA-2021:2308)	Vulnerability - level 4	Vuln
960003	Rocky Linux Security Update for kernel-rt (RLSA-2021:4646)	Vulnerability - level 5	Vuln
960016	Rocky Linux Security Update for libxml2 (RLSA-2021:2569)	Vulnerability - level 4	Vuln
960049	Rocky Linux Security Update for bind (RLSA-2021:1989)	Vulnerability - level 4	Vuln
960053	Rocky Linux Security Update for postgresql:9.6 (RLSA-2021:2360)	Vulnerability - level 4	Vuln
960090	Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2021:5226)	Vulnerability - level 4	Vuln
960091	Rocky Linux Security Update for postgresql:13 (RLSA-2021:2375)	Vulnerability - level 4	Vuln
960093	Rocky Linux Security Update for postgresql:12 (RLSA-2021:2372)	Vulnerability - level 4	Vuln
960094	Rocky Linux Security Update for kernel (RLSA-2021:4647)	Vulnerability - level 5	Vuln
960101	Rocky Linux Security Update for postgresql:10 (RLSA-2021:2361)	Vulnerability - level 4	Vuln
960157	Rocky Linux Security Update for kernel-rt (RLSA-2022:5565)	Vulnerability - level 4	Vuln
960158	Rocky Linux Security Update for kernel (RLSA-2022:5564)	Vulnerability - level 4	Vuln
960175	Rocky Linux Security Update for httpd:2.4 (RLSA-2022:7647)	Vulnerability - level 5	Vuln
960176	Rocky Linux Security Update for kernel-rt (RLSA-2022:7444)	Vulnerability - level 4	Vuln
960184	Rocky Linux Security Update for kernel (RLSA-2022:7683)	Vulnerability - level 4	Vuln
960189	Rocky Linux Security Update for nodejs:14 (RLSA-2022:6448)	Vulnerability - level 4	Vuln
960205	Rocky Linux Security Update for bind (RLSA-2022:7790)	Vulnerability - level 3	Vuln
960214	Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2022:5818)	Vulnerability - level 5	Vuln
960225	Rocky Linux Security Update for nghttp2 (RLSA-2020:2755)	Vulnerability - level 4	Vuln
960230	Rocky Linux Security Update for nodejs:12 (RLSA-2020:4272)	Vulnerability - level 4	Vuln
960271	Rocky Linux Security Update for kernel-rt (RLSA-2022:7134)	Vulnerability - level 4	Vuln
960277	Rocky Linux Security Update for nodejs:16 (RLSA-2022:6449)	Vulnerability - level 4	Vuln
960283	Rocky Linux Security Update for bind (RLSA-2022:2092)	Vulnerability - level 3	Vuln
960296	Rocky Linux Security Update for e2fsprogs (RLSA-2022:7720)	Vulnerability - level 4	Vuln
960300	Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2022:5337)	Vulnerability - level 4	Vuln
960324	Rocky Linux Security Update for httpd:2.4 (RLSA-2022:1049)	Vulnerability - level 5	Vuln
960340	Rocky Linux Security Update for idm:DL1 and idm:client (RLSA-2020:4670)	Vulnerability - level 3	Vuln
960345	Rocky Linux Security Update for libvncserver (RLSA-2021:1811)	Vulnerability - level 4	Vuln
960354	Rocky Linux Security Update for nodejs:12 (RLSA-2020:2852)	Vulnerability - level 4	Vuln
960359	Rocky Linux Security Update for sqlite (RLSA-2021:4396)	Vulnerability - level 4	Vuln
960394	Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2022:1819)	Vulnerability - level 5	Vuln
960397	Rocky Linux Security Update for kernel (RLSA-2022:7110)	Vulnerability - level 4	Vuln
960425	Rocky Linux Security Update for nodejs:10 (RLSA-2020:2848)	Vulnerability - level 4	Vuln

960440	Rocky Linux Security Update for httpd:2.4 (RLSA-2021:3816)	Vulnerability - level 5	Vuln
960442	Rocky Linux Security Update for expat (RLSA-2022:5314)	Vulnerability - level 4	Vuln
960443	Rocky Linux Security Update for subversion:1.10 (RLSA-2019:2512)	Vulnerability - level 4	Vuln
960454	Rocky Linux Security Update for pki-core:10.6 and pki-deps:10.6 (RLSA-2020:4847)	Vulnerability - level 3	Vuln
960456	Rocky Linux Security Update for bind9.16 (RLSA-2022:7643)	Vulnerability - level 3	Vuln
960461	Rocky Linux Security Update for shim (RLSA-2021:1734)	Vulnerability - level 4	Vuln
960481	Rocky Linux Security Update for httpd (RLSA-2022:8067)	Vulnerability - level 5	Vuln
960531	Rocky Linux Security Update for nodejs and nodejs-nodemon (RLSA-2022:6595)	Vulnerability - level 5	Vuln
960562	Rocky Linux Security Update for dhcp (RLSA-2022:8385)	Vulnerability - level 3	Vuln
960566	Rocky Linux Security Update for xmlrpc-c (RLSA-2022:1643)	Vulnerability - level 5	Vuln
960592	Rocky Linux Security Update for e2fsprogs (RLSA-2022:8361)	Vulnerability - level 4	Vuln
960612	Rocky Linux Security Update for go-toolset and golang (RLSA-2022:5799)	Vulnerability - level 4	Vuln
960622	Rocky Linux Security Update for xmlrpc-c (RLSA-2022:7692)	Vulnerability - level 5	Vuln
960628	Rocky Linux Security Update for bind (RLSA-2022:8068)	Vulnerability - level 3	Vuln
960691	Rocky Linux Security Update for grafana (RLSA-2022:0001)	Vulnerability - level 4	Vuln
960698	Rocky Linux Security Update for edk2 (RLSA-2021:4198)	Vulnerability - level 4	Vuln
960703	Rocky Linux Security Update for nodejs:12 (RLSA-2021:0734)	Vulnerability - level 4	Vuln
960723	Rocky Linux Security Update for httpd:2.4 (RLSA-2022:0891)	Vulnerability - level 5	Vuln
960737	Rocky Linux Security Update for microcode_ctl (RLSA-2021:3027)	Vulnerability - level 4	Vuln
960740	Rocky Linux Security Update for curl (RLSA-2021:1610)	Vulnerability - level 4	Vuln
960743	Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2021:4156)	Vulnerability - level 4	Vuln
960746	Rocky Linux Security Update for pcs (RLSA-2021:4142)	Vulnerability - level 3	Vuln
960759	Rocky Linux Security Update for pki-deps:10.6 (RLSA-2019:1529)	Vulnerability - level 5	Vuln
960760	Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2021:5160)	Vulnerability - level 4	Vuln
960795	Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2021:4424)	Vulnerability - level 4	Vuln
960796	Rocky Linux Security Update for subversion:1.10 (RLSA-2020:4712)	Vulnerability - level 3	Vuln
960820	Rocky Linux Security Update for libxml2 (RLSA-2022:0899)	Vulnerability - level 4	Vuln
960826	Rocky Linux Security Update for fwupd (RLSA-2021:2566)	Vulnerability - level 4	Vuln
960827	Rocky Linux Security Update for nodejs:14 (RLSA-2021:0744)	Vulnerability - level 4	Vuln
960832	Rocky Linux Security Update for thunderbird (RLSA-2022:0845)	Vulnerability - level 5	Vuln
960834	Rocky Linux Security Update for firefox (RLSA-2022:0818)	Vulnerability - level 5	Vuln
960838	Rocky Linux Security Update for bind (RLSA-2021:4384)	Vulnerability - level 3	Vuln
960839	Rocky Linux Security Update for nodejs:10 (RLSA-2021:0735)	Vulnerability - level 4	Vuln
960843	Rocky Linux Security Update for nodejs:10 (RLSA-2021:0548)	Vulnerability - level 5	Vuln
960848	Rocky Linux Security Update for expat (RLSA-2022:0951)	Vulnerability - level 5	Vuln
960853	Rocky Linux Security Update for python27:2.7 (RLSA-2019:0981)	Vulnerability - level 5	Vuln
960860	Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2021:1024)	Vulnerability - level 4	Vuln
960863	Rocky Linux Security Update for nodejs:14 (RLSA-2022:0350)	Vulnerability - level 5	Vuln
960886	Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2023:1405)	Vulnerability - level 4	Vuln
960889	Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2023:0946)	Vulnerability - level 4	Vuln
980093	Go (go) Security Update for github.com/containerd/containerd (GHSA-c2h3-6mxw-7mvq)	Vulnerability - level 3	Vuln
980150	Nodejs (npm) Security Update for tar (GHSA-9r2w-394v-53qc)	Vulnerability - level 4	Vuln
980152	Nodejs (npm) Security Update for tar (GHSA-qq89-hq3f-393p)	Vulnerability - level 4	Vuln
980287	Nodejs (npm) Security Update for jquery (GHSA-6c3j-c64m-qhgg)	Vulnerability - level 3	Vuln
980365	Nodejs (npm) Security Update for tar (GHSA-r628-mhmq-qjhw)	Vulnerability - level 4	Vuln
980366	Nodejs (npm) Security Update for tar (GHSA-3jfq-g458-7qm9)	Vulnerability - level 4	Vuln
980369	Nodejs (npm) Security Update for tar (GHSA-5955-9wpr-37jh)	Vulnerability - level 4	Vuln
980370	Nodejs (npm) Security Update for @npmcli/arborist (GHSA-2h3h-q99f-3fhc)	Vulnerability - level 3	Vuln

980371	Nodejs (npm) Security Update for @npmcli/arborist2 (GHSA-gmw6-94gg-2rc2)	Vulnerability - level 3	Vuln
980772	Nodejs (npm) Security Update for cordova-plugin-ionic-webview (GHSA-xwjh-cp99-cj8q)	Vulnerability - level 4	Vuln
980827	Python (pip) Security Update for ansible (GHSA-w578-j992-554x)	Vulnerability - level 5	Vuln
980894	Java (maven) Security Update for org.apache.tomcat.embed:tomcat-embed-core (GHSA-r4x2-3cq5-hqvp)	Vulnerability - level 5	Vuln
980943	Java (maven) Security Update for org.apache.qpid:qpid-broker-plugins-amqp-1-0-protocol (GHSA-q66c-h853-gqw2)	Vulnerability - level 5	Vuln
981010	Java (maven) Security Update for org.apache.qpid:qpid-broker (GHSA-jj9h-mwhq-8vhm)	Vulnerability - level 3	Vuln
981078	DotNet (Nuget) Security Update for OPCFoundation.NetStandard.Opc.Ua (GHSA-gr4c-5rq6-cgh3)	Vulnerability - level 3	Vuln
981115	Java (maven) Security Update for org.apache.qpid:proton-j (GHSA-f5cf-f7px-xpmh)	Vulnerability - level 3	Vuln
981212	Java (maven) Security Update for org.eclipse.jetty:jetty-server (GHSA-872g-2h8h-362q)	Vulnerability - level 5	Vuln
981216	Java (maven) Security Update for org.apache.hive:hive-service (GHSA-83r3-c79w-f6wc)	Vulnerability - level 4	Vuln
981306	Java (maven) Security Update for org.apache.tika:tika-core (GHSA-4xr4-4c65-hj7f)	Vulnerability - level 4	Vuln
981324	Java (maven) Security Update for org.apache.pdfbox:pdfbox (GHSA-4c32-xmgj-2g98)	Vulnerability - level 4	Vuln
981332	Nodejs (npm) Security Update for moment (GHSA-446m-mv8f-q348)	Vulnerability - level 4	Vuln
981402	Java (maven) Security Update for org.apache.httpcomponents:httpClient (GHSA-2x83-r56g-cv47)	Vulnerability - level 2	Vuln
981983	Nodejs (npm) Security Update for bootstrap (GHSA-3mgp-fx93-9xv5)	Vulnerability - level 3	Vuln
981996	Java (maven) Security Update for org.apache.taglibs:taglibs-standard-impl (GHSA-6x4w-8w53-xrvv)	Vulnerability - level 2	Vuln
984159	Java (maven) Security Update for org.springframework:spring-core (GHSA-558x-2xjg-6232)	Vulnerability - level 3	Vuln
984162	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-76vr-72mv-mf3q)	Vulnerability - level 3	Vuln
984163	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-jgm2-m5cg-f66g)	Vulnerability - level 3	Vuln
984164	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-55j7-f5wf-43m4)	Vulnerability - level 4	Vuln
984165	Java (maven) Security Update for org.apache.hadoop:hadoop-client (GHSA-qmh2-h7r6-gm6q)	Vulnerability - level 4	Vuln
984167	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-76vr-72mv-mf3q)	Vulnerability - level 3	Vuln
984168	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-jgm2-m5cg-f66g)	Vulnerability - level 3	Vuln
984169	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-55j7-f5wf-43m4)	Vulnerability - level 4	Vuln
984170	Java (maven) Security Update for org.apache.hadoop:hadoop-client (GHSA-qmh2-h7r6-gm6q)	Vulnerability - level 4	Vuln
984172	Java (maven) Security Update for org.apache.commons:commons-compress (GHSA-6fxm-66hq-fc96)	Vulnerability - level 3	Vuln
984173	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-vjpc-vf4f-82qg)	Vulnerability - level 3	Vuln
984192	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-76vr-72mv-mf3q)	Vulnerability - level 3	Vuln
984193	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-jgm2-m5cg-f66g)	Vulnerability - level 3	Vuln

984194	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-55j7-f5wf-43m4)	Vulnerability - level 4	Vuln
984195	Java (maven) Security Update for org.apache.hadoop:hadoop-client (GHSA-qmh2-h7r6-gm6q)	Vulnerability - level 4	Vuln
984197	Java (maven) Security Update for org.apache.commons:commons-compress (GHSA-6fxm-66hq-fc96)	Vulnerability - level 3	Vuln
984198	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-vjpc-vf4f-82qg)	Vulnerability - level 3	Vuln
984229	Java (maven) Security Update for org.springframework.security:spring-security-core (GHSA-4644-hg35-55m9)	Vulnerability - level 3	Vuln
984248	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-xf9f-32gh-h2w4)	Vulnerability - level 3	Vuln
984271	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-76vr-72mv-mf3q)	Vulnerability - level 3	Vuln
984272	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-jgm2-m5cg-f66g)	Vulnerability - level 3	Vuln
984273	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-55j7-f5wf-43m4)	Vulnerability - level 4	Vuln
984274	Java (maven) Security Update for org.apache.hadoop:hadoop-client (GHSA-qmh2-h7r6-gm6q)	Vulnerability - level 4	Vuln
984276	Java (maven) Security Update for org.apache.commons:commons-compress (GHSA-6fxm-66hq-fc96)	Vulnerability - level 3	Vuln
984277	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-vjpc-vf4f-82qg)	Vulnerability - level 3	Vuln
984305	Java (maven) Security Update for org.springframework.security:spring-security-core (GHSA-4644-hg35-55m9)	Vulnerability - level 3	Vuln
984324	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-xf9f-32gh-h2w4)	Vulnerability - level 3	Vuln
984428	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-76vr-72mv-mf3q)	Vulnerability - level 3	Vuln
984429	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-jgm2-m5cg-f66g)	Vulnerability - level 3	Vuln
984430	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-55j7-f5wf-43m4)	Vulnerability - level 4	Vuln
984431	Java (maven) Security Update for org.apache.hadoop:hadoop-client (GHSA-qmh2-h7r6-gm6q)	Vulnerability - level 4	Vuln
984433	Java (maven) Security Update for org.apache.commons:commons-compress (GHSA-6fxm-66hq-fc96)	Vulnerability - level 3	Vuln
984434	Java (maven) Security Update for org.apache.cxf:cxf (GHSA-vjpc-vf4f-82qg)	Vulnerability - level 3	Vuln
984462	Java (maven) Security Update for org.springframework.security:spring-security-core (GHSA-4644-hg35-55m9)	Vulnerability - level 3	Vuln
985325	Go (go) Security Update for github.com/docker/docker (GHSA-8w94-cf6g-c8mg)	Vulnerability - level 3	Vuln
985341	Go (go) Security Update for github.com/docker/docker (GHSA-44gg-pmqr-4669)	Vulnerability - level 3	Vuln
985407	Go (go) Security Update for github.com/docker/docker (GHSA-5qgp-p5jc-w2rm)	Vulnerability - level 4	Vuln
985579	Java (maven) Security Update for org.apache.geronimo.framework:geronimo-jmx-remoting (GHSA-v64w-96p6-fx7w)	Vulnerability - level 4	Vuln
985733	Python (pip) Security Update for pyamf (GHSA-m7m4-4vm8-55wg)	Vulnerability - level 4	Vuln
985832	Nodejs (npm) Security Update for electron (GHSA-mq8j-3h7h-p8g7)	Vulnerability - level 2	Vuln

986426	Java (maven) Security Update for org.apache.shiro:shiro-core (GHSA-4cf5-xmhp-3xj7)	Vulnerability - level 5	Vuln
986435	Java (maven) Security Update for org.apache.hadoop:hadoop-common (GHSA-pxv5-5vmp-3jj4)	Vulnerability - level 2	Vuln
986438	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-6m48-jxwx-76q7)	Vulnerability - level 3	Vuln
986442	Java (maven) Security Update for org.apache.openjpa:openjpa (GHSA-j65f-mvgw-prp2)	Vulnerability - level 4	Vuln
986444	Java (maven) Security Update for commons-fileupload:commons-fileupload (GHSA-vm69-474v-7q2w)	Vulnerability - level 2	Vuln
986445	Java (maven) Security Update for org.apache.cxf:cxf-rt-frontend-jaxrs (GHSA-p5c5-6564-vvr8)	Vulnerability - level 3	Vuln
986452	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-fj6c-prgj-gr3r)	Vulnerability - level 2	Vuln
986457	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-87w9-x2c3-hrjj)	Vulnerability - level 3	Vuln
986462	Java (maven) Security Update for org.springframework:spring-web (GHSA-xjrf-8x4f-43h4)	Vulnerability - level 3	Vuln
986463	Java (maven) Security Update for org.springframework:spring-web (GHSA-g6hf-f9cq-q7w7)	Vulnerability - level 3	Vuln
986464	Java (maven) Security Update for org.opensaml:opensaml (GHSA-v723-58jv-2qc4)	Vulnerability - level 3	Vuln
986468	Java (maven) Security Update for org.springframework:spring-webmvc (GHSA-8cmm-qj8g-fcp6)	Vulnerability - level 3	Vuln
986472	Java (maven) Security Update for org.springframework.security:spring-security-core (GHSA-gv9v-c375-hvmg)	Vulnerability - level 4	Vuln
986480	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-6gjj-c5mj-4cvp)	Vulnerability - level 3	Vuln
986481	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-qprx-q2r7-3rx6)	Vulnerability - level 3	Vuln
986483	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-prc3-7f44-w48j)	Vulnerability - level 3	Vuln
986484	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-42j3-498q-m6vp)	Vulnerability - level 3	Vuln
986490	Java (maven) Security Update for org.apache.poi:poi (GHSA-q56h-jjj6-52mf)	Vulnerability - level 3	Vuln
986499	Java (maven) Security Update for org.apache.activemq:activemq-client (GHSA-72m6-23ff-7q26)	Vulnerability - level 4	Vuln
986501	Java (maven) Security Update for org.apache.hadoop:hadoop-client (GHSA-jpmf-8cj2-595g)	Vulnerability - level 3	Vuln
986508	Java (maven) Security Update for org.apache.activemq:activemq-client (GHSA-9cvr-8xq4-2m73)	Vulnerability - level 3	Vuln
986513	Java (maven) Security Update for org.apache.cassandra:apache-cassandra (GHSA-w7f2-gjxf-2gm9)	Vulnerability - level 4	Vuln
986530	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-6qr6-x7jm-x2q6)	Vulnerability - level 3	Vuln
986541	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-6vx3-hr43-cfrh)	Vulnerability - level 3	Vuln
986542	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-mv42-px54-87jw)	Vulnerability - level 4	Vuln
986548	Java (maven) Security Update for org.apache.struts:struts-core (GHSA-7jw3-5q4w-89qg)	Vulnerability - level 4	Vuln
986549	Java (maven) Security Update for org.apache.struts:struts-core (GHSA-5ggr-mpgw-3mgx)	Vulnerability - level 4	Vuln
986578	Java (maven) Security Update for org.apache.tomcat:tomcat-catalina (GHSA-v646-rx6w-r3qq)	Vulnerability - level 4	Vuln
986669	Java (maven) Security Update for org.apache.hadoop:hadoop-client (GHSA-pr9x-qmp5-j3rr)	Vulnerability - level 4	Vuln

986782	Java (maven) Security Update for org.apache.poi:poi (GHSA-5wfp-8643-c58x)	Vulnerability - level 3	Vuln
987182	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-8wch-9gcg-v2pr)	Vulnerability - level 3	Vuln
987183	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-hhjg-g8xq-hhr3)	Vulnerability - level 3	Vuln
987186	Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-hjfh-7c4v-7q8h)	Vulnerability - level 3	Vuln
987655	Rust (rust) Security Update for Open Secure Sockets Layer (OpenSSL-src) (GHSA-g323-fr93-4j3c)	Vulnerability - level 4	Vuln
987656	Rust (rust) Security Update for Open Secure Sockets Layer (OpenSSL-src) (GHSA-mfm6-r9g2-q4r7)	Vulnerability - level 3	Vuln
987657	Rust (rust) Security Update for Open Secure Sockets Layer (OpenSSL-src) (GHSA-638m-m8mh-7gw2)	Vulnerability - level 3	Vuln
988118	Rust (Rust) Security Update for Open Secure Sockets Layer (OpenSSL-src) (GHSA-5ww6-px42-wc85)	Vulnerability - level 5	Vuln
988210	Rubygems (Rubygems) Security Update for nokogiri (GHSA-7553-jr98-vx47)	Vulnerability - level 4	Vuln
988231	Rust (Rust) Security Update for Open Secure Sockets Layer (OpenSSL-src) (GHSA-3wx7-46ch-7rq2)	Vulnerability - level 4	Vuln
988285	Rust (Rust) Security Update for Open Secure Sockets Layer (OpenSSL-src) (GHSA-q9wj-f4qw-6vfj)	Vulnerability - level 4	Vuln
988440	PHP (Composer) Security Update for guzzlehttp/guzzle (GHSA-m6ch-gg5f-wxx3)	Vulnerability - level 4	Vuln
988558	Rubygems (Rubygems) Security Update for activerecord (GHSA-3crr-9vmg-864v)	Vulnerability - level 3	Vuln
988586	Rubygems (Rubygems) Security Update for passenger (GHSA-9qj7-jvg4-qr2x)	Vulnerability - level 3	Vuln
988601	Rubygems (Rubygems) Security Update for activesupport (GHSA-9c2j-593q-3g82)	Vulnerability - level 3	Vuln
988650	Rubygems (Rubygems) Security Update for activesupport (GHSA-h835-75hw-pj89)	Vulnerability - level 3	Vuln
988668	Rubygems (Rubygems) Security Update for actionpack (GHSA-98mf-8f57-64qf)	Vulnerability - level 3	Vuln
988673	Rubygems (Rubygems) Security Update for actionpack (GHSA-7cgp-c3g7-qvrw)	Vulnerability - level 3	Vuln
988700	Rubygems (Rubygems) Security Update for actionpack (GHSA-7g65-ghrg-hpf5)	Vulnerability - level 3	Vuln
988763	Rust (Rust) Security Update for openssl-src (GHSA-qgm6-9472-pwq7)	Vulnerability - level 4	Vuln
988788	Rust (Rust) Security Update for openssl-src (GHSA-83mx-573x-5rw9)	Vulnerability - level 3	Vuln
988793	Rust (Rust) Security Update for openssl-src (GHSA-84rm-qf37-fgc2)	Vulnerability - level 3	Vuln
988805	Rust (Rust) Security Update for openssl-src (GHSA-8hfj-xrj2-pm22)	Vulnerability - level 4	Vuln
989149	Rubygems (Rubygems) Security Update for actionpack (GHSA-j838-vfpq-fmf2)	Vulnerability - level 3	Vuln
989173	Rubygems (Rubygems) Security Update for actionpack (GHSA-q759-hwvc-m3jg)	Vulnerability - level 3	Vuln
989195	Rubygems (Rubygems) Security Update for cocaine (GHSA-c43v-hrmg-56r4)	Vulnerability - level 3	Vuln
990014	Java (Maven) Security Update for org.apache.openmeetings:openmeetings-parent (GHSA-gw38-mxr2-rm8r)	Vulnerability - level 3	Vuln
990095	Java (Maven) Security Update for org.apache.openmeetings:openmeetings-parent (GHSA-f6vf-465r-h42p)	Vulnerability - level 4	Vuln

990245	Java (Maven) Security Update for org.apache.santuario:xmlsec (GHSA-8hfm-837h-hjg5)	Vulnerability - level 3	Vuln
990249	Java (Maven) Security Update for org.jruby:jruby (GHSA-hgg7-cghq-xhf4)	Vulnerability - level 3	Vuln
990396	Java (Maven) Security Update for org.apache.nifi:nifi (GHSA-g2fm-x3cp-mqw9)	Vulnerability - level 3	Vuln
990458	Java (Maven) Security Update for org.elasticsearch:elasticsearch (GHSA-8699-m855-cwqf)	Vulnerability - level 3	Vuln
992009	GO (Go) Security Update for golang.org/x/net/http2 (GHSA-vc3p-29h2-gpcp)	Vulnerability - level 4	Vuln
992059	Python (Pip) Security Update for keystone (GHSA-22q6-wwq7-2jj9)	Vulnerability - level 3	Vuln
992068	Python (Pip) Security Update for cryptography (GHSA-x4qr-2fvf-3mr5)	Vulnerability - level 3	Vuln
992099	Rust (Rust) Security Update for openssl-src (GHSA-x4qr-2fvf-3mr5)	Vulnerability - level 3	Vuln
992100	Rust (Rust) Security Update for openssl-src (GHSA-v5w6-wcm8-jm4q)	Vulnerability - level 3	Vuln
992102	Rust (Rust) Security Update for openssl-src (GHSA-r7jw-wp68-3xch)	Vulnerability - level 3	Vuln
992106	Rust (Rust) Security Update for openssl-src (GHSA-p52g-cm5j-mjv4)	Vulnerability - level 3	Vuln
992405	Java (Maven) Security Update for org.apache.tomcat:tomcat (GHSA-3xpj-jgv5-q4vv)	Vulnerability - level 3	Vuln
992406	Java (Maven) Security Update for org.apache.tomcat:tomcat (GHSA-p26v-97vp-jcx6)	Vulnerability - level 3	Vuln
992426	Rubygems (Rubygems) Security Update for nokogiri (GHSA-jw9f-hh49-cvp9)	Vulnerability - level 4	Vuln
992429	Rubygems (Rubygems) Security Update for rubygems-update (GHSA-9j7m-rjqx-48vh)	Vulnerability - level 3	Vuln
992433	Rubygems (Rubygems) Security Update for ruby_parser (GHSA-8mvw-22r7-w6fq)	Vulnerability - level 2	Vuln
992443	Rubygems (Rubygems) Security Update for rubygems-update (GHSA-wp3j-rvfp-624h)	Vulnerability - level 4	Vuln
992639	Python (Pip) Security Update for redis (GHSA-24wv-mv5m-xv4h)	Vulnerability - level 4	Vuln
993232	Rubygems (Rubygems) Security Update for jquery-rails (GHSA-6c3j-c64m-qhgq)	Vulnerability - level 3	Vuln
993257	DotNet (Nuget) Security Update for jQuery (GHSA-6c3j-c64m-qhgq)	Vulnerability - level 3	Vuln