



Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.20

July 22, 2022

This new release of the Qualys Cloud Platform (VM, PC) includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

[MongoDB Authentication: Certificates/Private Keys Now Supported With Basic and Vault Login](#)

Qualys Policy Compliance (PC/SCAP/SCA)

[New Authentication Support for Infoblox](#)

[New Technology Support: Mac Apple Safari 12.x/13.x/14.x/15.x \(Agent\)](#)

Qualys Vulnerability Management (VM)

[Set Maximum Scan Duration per Asset](#)

[Schedules Data List Setup](#)

[Display CVSS Version 3.1](#)

[CVSSv2 Score Appears in Host Based Scan Reports Without Asset Groups](#)

[Show/Hide TruRisk Details \(ARS, ACS, QDS\) in Scan Reports](#)

API Changes

Refer to the [Cloud Platform 10.20 API Release Notes](#) for API changes in this release.

Qualys 10.20 brings you many more improvements and updates! [Learn more](#)

Qualys Cloud Platform

MongoDB Authentication: Certificates/Private Keys Now Supported With Basic and Vault Login

Users can now pass Certificates/Private Keys (Optional) along with Basic & Vault-based login credentials. Previously, the MongoDB authentication record supported one of the 3 authentication types:

- Basic - Username and password-based
- Vault based - Username and Vault integration used for storing login credentials
- Private key/certificate based

Now, a new option called **Require Certificate** has been added to the MongoDB authentication record, which is visible for Basic and Vault-based login. This option is off by default (set to **NO**) but if you enable it (set to **YES**), then you'll be able to add private key and certificate details. Use this option if the server requires client certificates for password-based authentication.

Good to Know

- The Require Certificate option is available for both Local authentication & External LDAP authentication credential types, and for both Basic & Vault-based authentication types.
- Once you select the Require Certificate option, the Private Keys/Certificates fields will be enabled. With this option, username, password and certificates are mandatory.
- Users can still create MongoDB authentication records with Basic, Vault based or Private key/certificate based authentication without using the Require Certificate option and it will work the same as it did before.
- This new option is supported for vulnerability scans and compliance scans.

To use the new option, go to **Scans > Authentication > New > Databases > MongoDB**. You'll see the new option **Require Certificate**. It's set to **NO** by default. Toggle the button to **YES** to pass Private Keys/Certificates along with username & password for Basic & Vault-based login types.

New MongoDB Record

Record Title >

Login Credentials

Use the local authentication or choose to use external LDAP authentication for credential type.

Credential Type: ☒ Local authentication ☐ External LDAP authentication

Authentication

Provide login credentials to use for authenticated scanning. Use the basic login credential or private key or choose to use authentication vault for authenticated scanning.

Authentication Type:

Require Certificate: ☐ NO ☐ YES

Select this option if the server is configured to require client certificates for the password-based authentication.

Username*:

Password*:

Confirm Password*:

MongoDB Authentication with Basic login type & Require Certificate option enabled

With the Require Certificate option enabled, the user can now pass Private Key, Passphrase & Certificate along with Username & Password for Basic & Vault login types.

The screenshot shows the 'New MongoDB Record' form. On the left is a sidebar with navigation links: Record Title, Login Credentials (highlighted), Target Configuration, Unix Configuration, IPs, and Comments. The main form area has a 'Credential Type' section with 'Local authentication' selected. Below this is the 'Authentication' section, which is highlighted with a red border. It contains the following fields and options:

- Authentication Type:** A dropdown menu set to 'Basic'.
- Require Certificate:** A section with the instruction 'Select this option if the server is configured to require client certificates for the password-based authentication.' and a 'YES' radio button selected.
- Username*:** A text input field.
- Password*:** A text input field.
- Confirm Password*:** A text input field.
- Private key:** A section with the label 'Get private key from vault?' and a 'NO' radio button selected.
- Private Key Content:** A large text area for pasting the private key.
- Get passphrase from vault:** A section with a 'NO' radio button selected.
- Passphrase:** A text input field.
- Certificate Content:** A large text area for pasting the certificate content.

At the bottom of the form are 'Cancel' and 'Create' buttons.

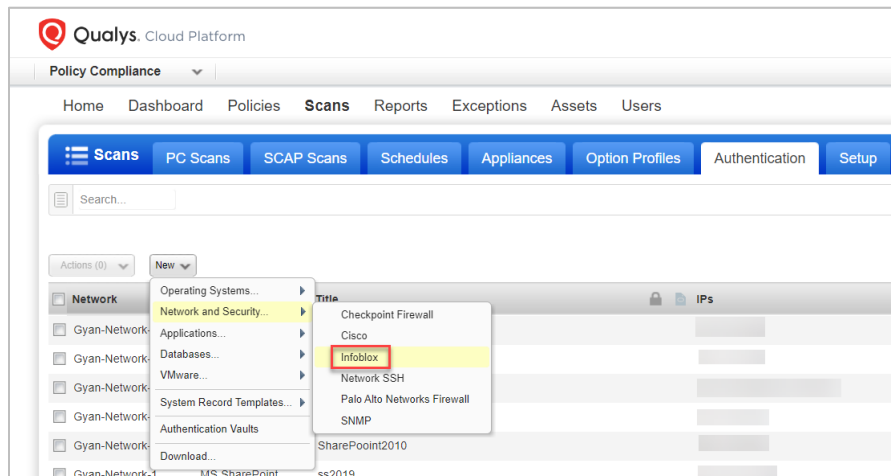
Qualys Policy Compliance (PC/SCAP/SCA)

New Authentication Support for Infoblox

We now support Infoblox authentication for compliance scans using Qualys apps PC, SCA. Simply create an Infoblox authentication record with details and scan it for compliance.

What are the steps?

Go to **Scans > Authentication > New > Network and Security > Infoblox**.



Your Infoblox authentication record

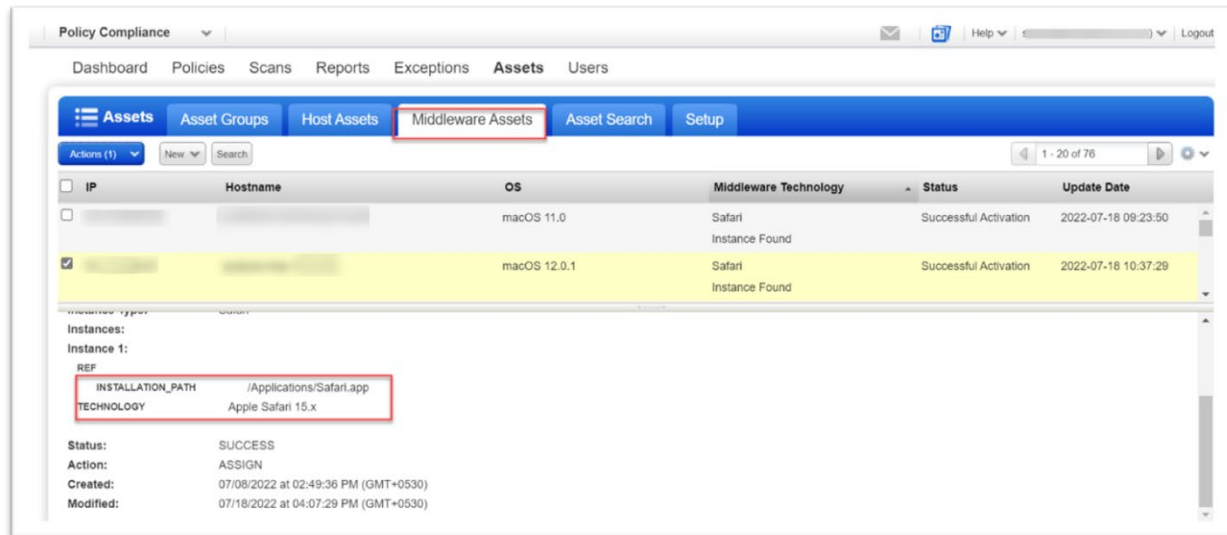
Each Infoblox record identifies account title, login credentials, API Version, and target hosts (IPs).

The screenshot shows the 'New Infoblox Record' form. On the left, there's a sidebar with a list of fields: 'Record Title', 'Login Credentials', 'API Version', 'IPs', and 'Comments'. The 'Record Title' field is expanded, showing a form with two input fields: 'Title*' and 'Network'. The 'Title*' field is empty, and the 'Network' field has a dropdown menu with 'Global Default Network' selected.

New Technology Support: Mac Apple Safari 12.x/13.x/14.x/15.x (Agent)

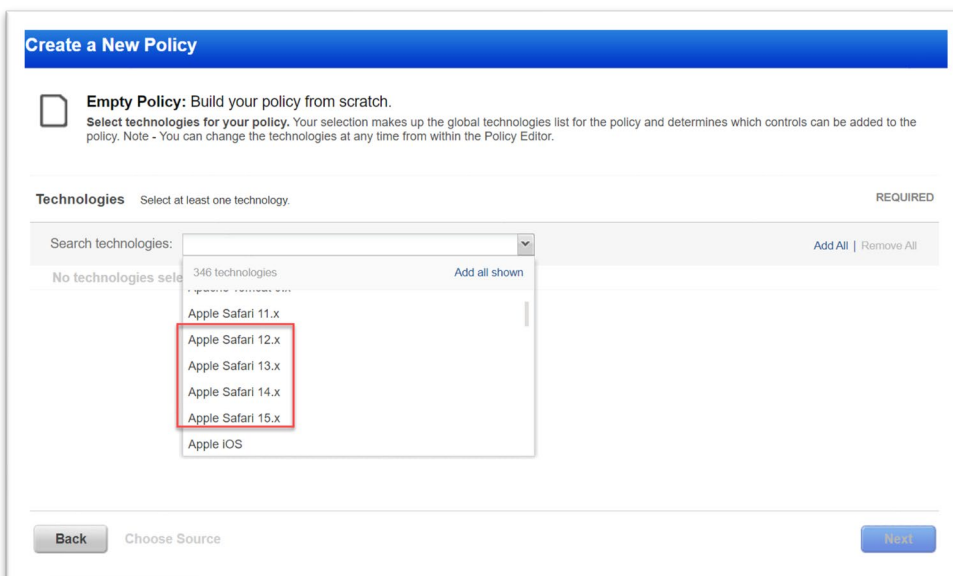
We have extended our support for Mac Apple Safari Server to include Apple Safari 12.x, 13.x, 14.x and 15.x. These Apple Safari technologies are supported for Agent scans.

If you are using Cloud Agent for Policy Compliance (PC), Apple Safari instances will be auto-discovered by the Cloud Agent. When an Apple Safari instance is detected on a host by an agent scan, it appears on the **PC > Assets > Middleware Assets** tab.



Policies and Controls

You'll see Apple Safari 12.x, 13.x, 14.x and 15.x in the **Technologies** list when creating new policies and when searching controls by technology.



You'll see the new technologies when searching controls under **Policies > Controls > Search**.

Search

CIDs:
Example: 1072, 1071, 1091 (up to 20)

Text:

Status: ☐ Deprecated

DB OS CIDs: ☐ Instance Data Collection

Technologies:

- ☐ Apple Safari 11.x
- ☐ Apple Safari 12.x
- ☐ Apple Safari 13.x
- ☐ Apple Safari 14.x
- ☐ Apple Safari 15.x
- ☐ Arista EOS 4.x

Frameworks:

- ☐ ANSSI 40 Essential Measures for a Healthy Network Ver 1.0
- ☐ APRA Prudential Practice Guide (PPG): CPG 234 - Manager
- ☐ CCI List 1
- ☐ CERT® Resilience Management Model 1.2

Search

Sample Report

You'll see instances of Apple Safari 12.x, 13.x, 14.x, 15.x technologies for scanned hosts in Scan Results and Compliance Reports. Here is a sample report with an instance of Apple Safari 15.x.

Detailed Results

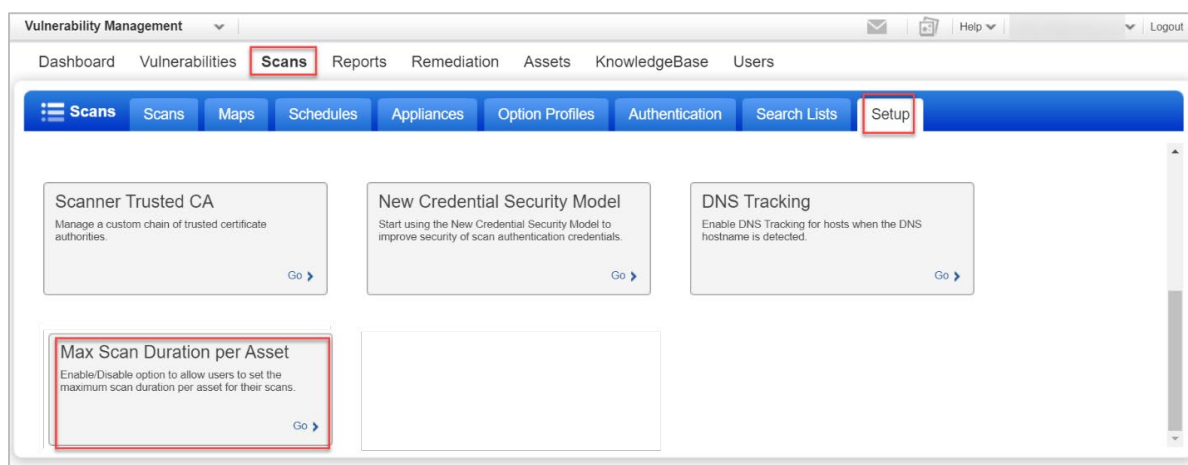
Qualys Vulnerability Management (VM)

Set Maximum Scan Duration per Asset

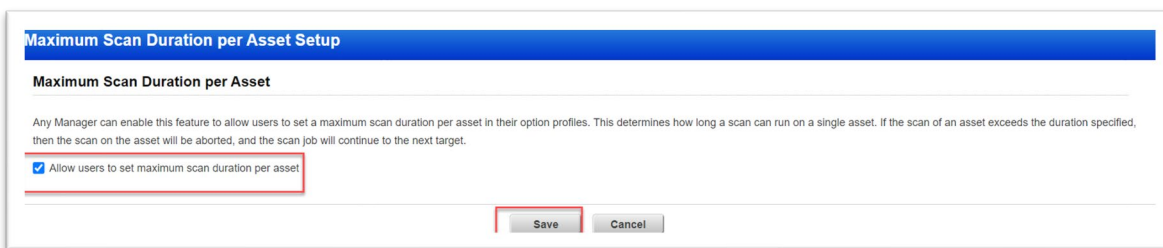
With this release, we have introduced the ability to set a maximum scan duration for how long a scan can run on a single asset. During the scanning process, if a slice spends more than the allowed time on a particular asset, then it will be skipped, and the scan will continue to conclusion for the remaining assets. The maximum scan time per asset is configured by the user in the Option Profile and the skipped asset will be displayed in Scan Summary. (Note that this scan setting is supported for vulnerability scans only.)

Enable the Maximum Scan Duration Feature (Manager Only)

A Manager can go to **Scans > Setup > Max Scan Duration per Asset** to enable/disable the feature that will allow users to set a maximum scan duration per asset for their scans.



In the window that opens, select the option **Allow users to set maximum scan duration per asset** and click **Save**. Once saved, users will see the new **Maximum Scan Duration per Asset** setting in their option profiles.



Set Maximum Scan Duration in Option Profile

Specify a maximum scan duration per asset for your scans. Go to **Scans > Option Profiles > New > Option Profile**. On the **Scan** tab, scroll to the **Maximum Scan Duration Per Asset** section. In the settings, select the option **Set maximum scan duration of <number> minutes per asset** and add the max duration in minutes (from 30 to 2880). Then click the **Save** button. When this feature is disabled or user has not defined any value in the option profile, this indicates that the scanner does not need to limit the time on any target.

Maximum Scan Duration per Asset

Set a limit on how long a scan can run on a single asset. If the scan of an asset exceeds the maximum scan duration specified, then the scan on the asset will be aborted, and the scan job will continue to the next target. .

☐ Set maximum scan duration of minutes per asset (30 to 2880 minutes).

View Option Profile Info

The **Option Profile Information** page will display the value set in the option profile for **Maximum Scan Duration per Asset**. On the **Option Profiles** tab, select **Info** from the **Quick Actions** menu for the option profile you are interested in. Click **Scan Settings** from the left panel and scan information is displayed.

Option Profile Information

General Information >

Scan Settings >

Map Settings >

System Authentication >

Additional Settings >

Scan Settings

Ports

Scanned TCP Ports: [Standard Scan](#)

Scanned UDP Ports: [Standard Scan](#)

Scan Dead Hosts: Off

Close Vulnerabilities on Dead Hosts Count: Off

Purge old host data when OS changes: Off

Load Balancer Detection: Off

Perform 3-way Handshake: Off

Vulnerability Detection : Complete

Intrusive Checks: Excluded

Password Brute Forcing

System: Disabled

Custom: Disabled

Maximum Scan Duration per Asset

Maximum Scan Duration Per Asset: 60 Minutes

Authentication

Windows: Disabled

Unix/Windows/Network OSs: Disabled

Close

Edit

View Scan Status

The assets that exceeded the maximum scan duration specified in the option profile will be listed in the **Scan Status** page. To view **Scan Status**, go to the **Scans** list and select the scan you're interested in. Then click **View Summary** in the **Preview Pane** below the data list.

The screenshot shows the Qualys Vulnerability Management interface. The top navigation bar includes 'Dashboard', 'Vulnerabilities', 'Scans', 'Reports', 'Remediation', 'Assets', 'KnowledgeBase', and 'Users'. The 'Scans' tab is selected, and a sub-menu is open with options like 'Maps', 'Schedules', 'Appliances', 'Option Profiles', 'Authentication', 'Search Lists', and 'Setup'. Below this, there's a table of scans. The first scan, 'VM_Schedule', is highlighted. Below the table, the 'Preview' pane is visible, showing details for 'Vulnerability Scan - VM_Schedule'. It includes the target '5 IP(s)', the network 'Global Default Network', and the scan status 'Scan Finished (00:31:10)'. A summary section shows 'Total Hosts Alive: 5', 'Total appliances used: 1', and 'Aggregate Vulnerabilities: 69'. A red box highlights the 'View Summary' button.

The **Scan Status** page appears. Click the **Hosts Exceeded Duration** tab on the left side. This will show a list of hosts that exceeded the maximum scan duration specified in the option profile. Hosts will be organized by target type: IPv4, IPv6, FQDN, NetBIOS. This tab will be blank if no hosts in the scan target exceeded scan duration. Note that you will not have any scan results for hosts that exceeded the scan duration.

The screenshot shows the 'Scan Status' page for scan/1657695823.49597. The left sidebar contains a list of tabs: 'General Information', 'Scanners', 'Option Profile', 'Targets', 'Failed Slice Host', and 'Hosts Exceeded Duration'. The 'Hosts Exceeded Duration' tab is selected and highlighted with a red box. The main content area shows a message: 'The scan was aborted for the following hosts because the scan exceeded the maximum scan duration per asset setting in the option profile. FQDNs : host1.sample.qualys.com, host2.sample.qualys.com, host3.sample.qualys.com'. A 'View Results' button is visible at the bottom right.

Schedules Data List Setup

With this release, we have introduced the ability to determine which schedules appear on the **Schedules** data list when it is first loaded. If the **Schedules** data list (under **Scans > Schedules**) takes too long to load, then a Manager user can use this option to display a filtered view of the list when it is first loaded. This setting applies to all users in the subscription. Users can apply filters or perform a search to find additional schedules.

Setup Settings

Go to **Scans > Setup > Schedules Data List Setup**. In the **Schedules Data List Setup** window that appears, select one of the options listed. You can choose to show all schedules, only active schedules, only VM scan schedules or only map schedules. Make your selection and click **Save**.

Schedules Data List Setup

Schedules Data List Setup

Any Manager can select from the options below to determine which schedules will appear on the Schedules data list when it's first loaded. This setting applies to all users in the subscription. Users can apply filters or perform a search to find additional schedules.

☐ All Schedules
Display all schedules initially.

☐ Active Schedules
Display only active schedules initially. Inactive schedules will not be shown.

☐ VM Scan Schedules
Display only scheduled scans initially. Map schedules will not be shown.

☒ Map Schedules
Display only scheduled maps initially. Scan schedules will not be shown.

Save Cancel

When you go to **Scans > Schedules** only the schedules that match your selection will appear in the list by default. In the example below, the **Map Schedules** option was selected on the **Schedules Data List Setup** page, so the list is filtered to show Map Tasks.

VMODR

Dashboard Vulnerabilities Prioritization **Scans** Reports Remediation Assets KnowledgeBase Users

Scans Scans Maps **Schedules** Appliances Option Profiles Authentication Search Lists Setup

Actions (0) New Search Filters Map Tasks

Type	Title	Targets	Scanner	Next Launch	Modified	Previous Duration
	8.10.x-Sch-Map	BIG_AG	External Scanner	12/15/2017 at 09:30:00 PM (GMT-0800)	12/15/2017 at 01:18:31 PM (GMT-0800)	00:07:30

Display CVSS Version 3.1

We already calculate CVSS3 scores for vulnerabilities based on CVSS version 3.1. However, the labels that appear in the UI, API and in Reports where we display CVSS3 scores did not reflect the 3.1 version number. Now you will see CVSS 3.1 when CVSS3 scores are displayed.

We updated CVSS3 labels to CVSS3.1 on the following UI screens and reports:

- Vulnerability Scan Results (all formats)
- Scan Report Template and Scan Reports (all formats)
- Patch Template and Patch Reports (all formats)
- PCI Scan Template and PCI Scan Reports (all formats)
- KnowledgeBase Column Headings
- KnowledgeBase Search
- Vulnerability Information
- Edit Vulnerability
- Dynamic Vulnerability Search List
- Static Vulnerability Search List

Note: As in previous releases, the CVSS Scoring feature must be enabled for the subscription to display CVSS scores for vulnerabilities. Managers enable CVSS Scoring for the subscription on the **CVSS Setup** page at **Reports > Setup > CVSS**.

Report Template

When CVSS Scoring is enabled for the subscription, you can choose to display CVSS scores in Scan Reports, Patch Reports and PCI Scan Reports. In the related report template, select the CVSS version you want to display: CVSSv2, CVSSv3.1 or All (both versions). The following sample is of a Scan Report Template but you'll see this change in Patch Report Templates and PCI Scan Report Templates too.

The screenshot shows the 'New Scan Report Template' dialog box. On the left is a sidebar with tabs: Report Title, Findings, Display (selected), Filter, Services and Ports, and User Access. The main area is divided into sections. The 'Sorting' section has a 'Sort by: *' dropdown set to 'Host'. The 'CVSS Version' section has a dropdown menu open, showing 'All' (selected), 'CVSSv2', and 'CVSSv3.1'. Below this is the 'Display Host Details' section with three checkboxes: 'Host Details' (unchecked), 'Host Asset Group Details' (unchecked), and 'Qualys System IDs' (unchecked). At the bottom is the 'Display Cloud Related Information' section with a 'Cloud Provider Metadata' checkbox (unchecked). At the bottom of the dialog are buttons for 'Cancel', 'Test', 'Save As...', and 'Save'. The top right corner has links for 'Turn help tips: On | Off' and 'Launch Help'.

Sample Reports

Here's a sample Host Based Scan Report in HTML format with CVSS3.1 scores.

Scan Report with CVSS3.1

File View Help

5 Oracle Java SE Critical Patch Update - April 2018 CVSS3.1: 7.2 New

First Detected:	05/02/2018 at 02:31:06 PM (GMT-0700)	Last Detected:	05/02/2018 at 02:31:06 PM (GMT-0700)	Times Detected:	1	Last Fixed:	N/A
QID:	370887	CVSS3.1 Base:	8.3	CVSS3.1 Temporal:	7.2		
Category:	Local						
Associated CVEs:	CVE-2018-2825 CVE-2018-2826 CVE-2018-2814 CVE-2018-2811 CVE-2018-2794 CVE-2018-2783 CVE-2018-2798 CVE-2018-2786 CVE-2018-2799 CVE-2018-2797 CVE-2018-2795 CVE-2018-2815 CVE-2018-2800 CVE-2018-2790						
Vendor Reference:	Oracle Java SE CPU April 2018						
Bugtraq ID:	103832 103877 103817 103847 103868 103846 103841 103872 103849 103810 103798 103848 103782 103796						
Service Modified:	12/09/2020						
User Modified:	-						
Edited:	No						
PCI Vuln:	Yes						
Ticket State:	Open						

Here's a sample Patch Report in Online format with CVSS3.1 scores.

Qualys Patch Report

Qualys Cloud Platform

Report Summary

Company: Qualys
Created by: [redacted]
Created on: 07/13/2022
Includes hosts scanned since 06/13/2022.
[View Report Targets...](#)

Total Patches	Hosts Requiring Patches	Vulnerabilities Addressed
306	1	306

HOSTS		PATCHES required on (306)	
IP	Netw... DNS R... NetBIOS OS OS CPE	Vendor ID	Sev... Title Published Values
Global	Oracle Enterprise Linux 8.0	ELSA-2019-096...	3 Oracle Enterprise Linux Security Update for edk2... 2 years ago 1 8.8
		ELSA-2019-097...	5 Oracle Enterprise Linux Security Update for cont... 2 years ago 1 8.6
		ELSA-2019-097...	3 Oracle Enterprise Linux Security Update for ghos... 2 years ago 1 7.8
		ELSA-2019-098...	4 Oracle Enterprise Linux Security Update for wget... 2 years ago 1 9.8
		ELSA-2019-114...	3 Oracle Enterprise Linux Security Update for bind... 2 years ago 1 7.5
		ELSA-2019-114...	3 Oracle Enterprise Linux Security Update for flatp... 2 years ago 1 9.0
		ELSA-2019-099...	3 Oracle Enterprise Linux Security Update for pyth... 2 years ago 1 9.8

In Vulnerability Scan Results you'll see CVSS3.1 scores. The other CVSS scores are for CVSSv2.

Scan Results

File View Help

1 ssh

Services

Detailed Results

(-) - Global Default Network Oracle Enterprise Linux 8.0
cpe:/o:oracle:oracle_linux:8.0::enterprise:

Vulnerabilities (2) [grid icon]

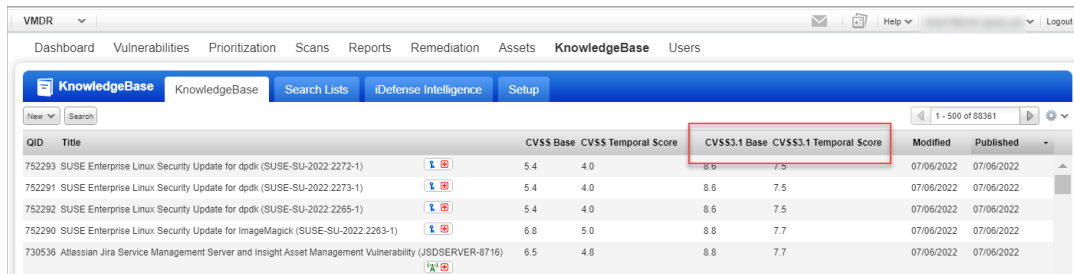
3 OpenSSH Command Injection Vulnerability (Generic)

QID:	105936	CVSS Base:	6.8
Category:	Security Policy	CVSS Temporal:	6.1
Associated CVEs:	CVE-2020-15778	CVSS3.1 Base:	7.8
Vendor Reference:	OpenSSH	CVSS3.1 Temporal:	7.4
Bugtraq ID:	-		
Service Modified:	08/05/2021		
User Modified:	-		
Edited:	No		
PCI Vuln:	Yes		

See [Cloud Platform 10.20 API Release Notes](#) for sample reports in XML and CSV formats.

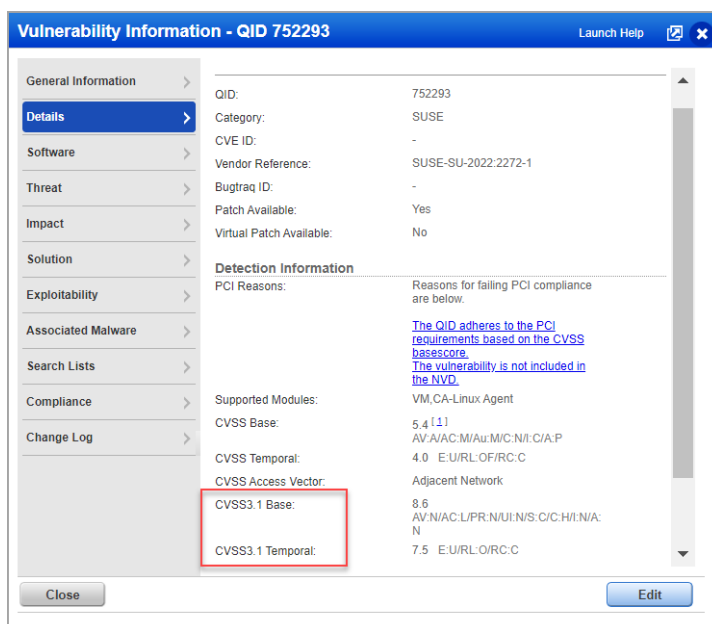
KnowledgeBase

In the **KnowledgeBase**, we renamed the CVSS3 column headings to CVSS3.1.



QID	Title	CVSS Base	CVSS Temporal Score	CVSS3.1 Base	CVSS3.1 Temporal Score	Modified	Published
752293	SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022-2272-1)	5.4	4.0	8.6	7.5	07/06/2022	07/06/2022
752291	SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022-2273-1)	5.4	4.0	8.6	7.5	07/06/2022	07/06/2022
752292	SUSE Enterprise Linux Security Update for dpdk (SUSE-SU-2022-2265-1)	5.4	4.0	8.6	7.5	07/06/2022	07/06/2022
752290	SUSE Enterprise Linux Security Update for ImageMagick (SUSE-SU-2022-2263-1)	6.8	5.0	8.8	7.7	07/06/2022	07/06/2022
730536	Atlassian Jira Service Management Server and Insight Asset Management Vulnerability (JSDSERVER-8716)	6.5	4.8	8.8	7.7	07/06/2022	07/06/2022

We renamed the CVSS3 Base and Temporal labels in Vulnerability Information to CVSS3.1.



Vulnerability Information - QID 752293

General Information

Details

Software

Threat

Impact

Solution

Exploitability

Associated Malware

Search Lists

Compliance

Change Log

QID: 752293

Category: SUSE

CVE ID: -

Vendor Reference: SUSE-SU-2022-2272-1

Bugtraq ID: -

Patch Available: Yes

Virtual Patch Available: No

Detection Information

PCI Reasons: Reasons for failing PCI compliance are below.

The QID adheres to the PCI requirements based on the CVSS basescore.

The vulnerability is not included in the NVD.

Supported Modules: VM,CA-Linux Agent

CVSS Base: 5.4 (1)

CVSS Temporal: 4.0 E:U/R/L:O/R/C

CVSS Access Vector: Adjacent Network

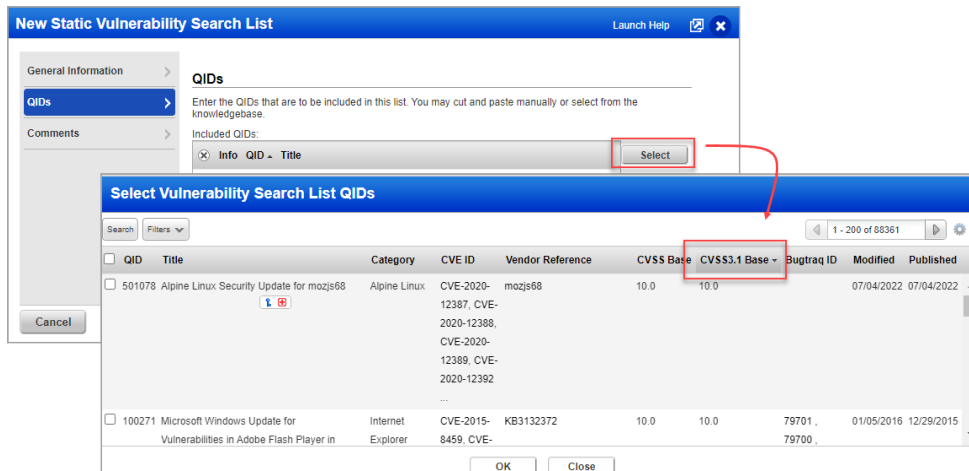
CVSS3.1 Base: 8.6

CVSS3.1 Temporal: 7.5 E:U/R/L:O/R/C

Close Edit

Search Lists

When you select QIDs for a Static Search List you'll see CVSS3.1 Base column.



New Static Vulnerability Search List

General Information

QIDs

Comments

Enter the QIDs that are to be included in this list. You may cut and paste manually or select from the knowledgebase.

Included QIDs:

Info QID Title Select

Select Vulnerability Search List QIDs

Search Filters

QID Title Category CVE ID Vendor Reference CVSS Base CVSS3.1 Base Bugtraq ID Modified Published

501078 Alpine Linux Security Update for mozilla Firefox 95.0.2 (CVE-2020-12387, CVE-2020-12388, CVE-2020-12389, CVE-2020-12392) 10.0 10.0 79701 07/04/2022 07/04/2022

100271 Microsoft Windows Update for Windows 10 (KB3132372) 10.0 10.0 79701 01/05/2016 12/29/2015

OK Close

When you select List Criteria for a Dynamic Search List you'll see CVSS3.1 labels.

CVSSv2 Score Appears in Host Based Scan Reports Without Asset Groups

Prior to this release, Host Based Scan Reports generated in CSV and XML formats would not show values for the final CVSSv2 score unless the report target included user-defined asset groups. Starting in this release, including asset groups in the report target is no longer required to see final CVSSv2 scores in your reports. The report target can include only IP addresses/ranges or the "All" asset group and you'll see the final CVSSv2 score.

CSV Reports

The **CVSS** column will now show final CVSSv2 scores instead of blank values. Note that values did appear in the **CVSS Base** and **CVSS Temporal** columns previously.

	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL
102															
103															
104															
105	Last Reopen	Times Reopened	CVE ID	Vendor Reference	Bugtraq ID	CVSS	CVSS Base	CVSS Temporal	CVSS Environment	CVSS3.1	CVSS3.1 Base	CVSS3.1 Temporal	Threat	Impact	Solution
106						3.9	4.3 (AV:N//3.9 (E:F/RL:W/F Asset Group: -, Coll			5	5.3 (AV:N/AC:H 5.0 (E:F/RL:W/R/C: The Web s			An attacke	Please
107						4.7	6.4 (AV:N//4.7 (E:U/RL:W/I Asset Group: -, Coll			5.3	6.5 (AV:N/AC:L 5.3 (E:U/RL:W/R/C: The SSH			A man-in-	Avoid
108						2	2.6 (AV:N//2.0 (E:U/RL:U/R Asset Group: -, Collateral Damage Potential: -, Target Distributi							The Web	If the brovCont
109			CVE-2002-0510		4314	4.8	5.0 (AV:N//4.8 (E:H/RL:U/R Asset Group: -, Collateral Damage Potential: -, Target Distributi							The host	By exploit We a
110						3.6	5.0 (AV:N//3.6 (E:U/RL:W/I Asset Group: -, Coll			4.4	5.3 (AV:N/AC:L 4.4 (E:U/RL:W/R/C: The SSH			A man-in-	DSA

XML Reports

The **<CVSS_FINAL>** tag will now show the final CVSSv2 score instead of a blank value.

```

...
<VULN_INFO>
  <QID id="qid_90527">90527</QID>
  <TYPE>Vuln</TYPE>
  <SSL>false</SSL>
  <RESULT><![CDATA[Microsoft SMB Remote Code Execution Vulnerability (KB975497) Detected]]></RESULT>
  <FIRST_FOUND>2022-03-07T09:10:06Z</FIRST_FOUND>
  <LAST_FOUND>2022-06-21T05:28:43Z</LAST_FOUND>
  <TIMES_FOUND>2</TIMES_FOUND>
  <VULN_STATUS>Active</VULN_STATUS>
  <CVSS_FINAL>8.7</CVSS_FINAL>
  <CVSS3_FINAL>9.5</CVSS3_FINAL>
  <CVSS3_VERSION>3.1</CVSS3_VERSION>
</VULN_INFO>
...

```

Show/Hide TruRisk Details (ARS, ACS, QDS) in Scan Reports

Applicable to subscriptions with the Asset Risk Scoring feature enabled.

Now you can control whether Qualys TruRisk details, including Asset Risk Score (ARS), Asset Criticality Score (ACS) and Qualys Detection Score (QDS), appear in Host Based Scan Reports. We've added a new scan report template option for displaying TruRisk details. This option is selected by default but you can clear it if you do not want to see TruRisk details in your reports.

How to display TruRisk details

1) Go to **VM/VMDR > Reports > Templates**. Create a new scan report template or edit an existing scan report template.

2) On the **Findings** tab, select **Host Based Findings**.

3) On the **Display** tab, select the following options:

- TruRisk Details (ARS, ACS, QDS)

- To see ARS and ACS in the report, you must also select **Text Summary** because these scores appear at the summary level for each host.

- To see QDS in the report, you must also select **Vulnerability Details** and at least one vulnerability detail like **Threat** because this score appears when you expand vulnerability details.

- Choose a **Sort by** option. When you sort by Host and TruRisk Details are included, then you'll see scores in all report formats: CSV, XML, HTML, DOCX, PDF and MHT. When you sort by some other method (e.g. Vulnerability, Operating System, Asset Group, etc) and TruRisk Details are included, you'll only see scores in CSV and XML report formats.

The screenshot shows the 'New Scan Report Template' window. On the left, the 'Display' tab is selected. The 'Sort by' dropdown is set to 'Host'. Under the 'Include the following detailed results in the report' section, the following options are checked: 'Text Summary', 'Vulnerability Details', 'Threat', and 'TruRisk Details (ARS, ACS, QDS)'. The 'TruRisk Details (ARS, ACS, QDS)' checkbox is highlighted with a red box. The 'Appendix' checkbox is unchecked. At the bottom, there are buttons for 'Cancel', 'Test', 'Save As...', and 'Save'.

Sample Scan Report

Here's a sample report in HTML format where the TruRisk details are shown in the report.

My Scan Report with TruRisk Details

File View Help

Detailed Results

▼ qvsa11.qualys.com (10.10.10.10 , -) - Test-Net CentOS 5.11
cpe:/o:centos:centos:5.11:::

Asset Risk Score: 709
Asset Criticality Score: 4

Total: 5 Security Risk: 3.4

by Severity	Confirmed	Potential	Information Gathered	Total
Severity				
5	1	-	-	1
4	1	-	-	1
3	2	-	-	2
2	1	-	-	1
1	0	-	-	0
Total	5	-	-	5

5 Biggest Categories	Confirmed	Potential	Information Gathered	Total
Category				
Security Policy	2	-	-	2
General remote services	2	-	-	2
CentOS	1	-	-	1
Total	5	-	-	5

▼ Vulnerabilities (5)

▼

5 EOL/Obsolete Operating System: CentOS 5.x Detected CVSS: 8.5 CVSS3.1: - Active

First Detected: 12/15/2021 at 11:06:23 PM (GMT-0800)

QID: 105713

Category: Security Policy

Associated CVEs: -

Vendor Reference: [CentOS 5 End of Life](#)

Bugtraq ID: -

Service Modified: 09/25/2019

User Modified: -

Edited: No

PCI Vuln: Yes

Ticket State: Open

QDS: 95

Last Detected: 04/18/2022 at 02:13:53 AM (GMT-0700)

CVSS Base: 10

CVSS Temporal: 8.5

CVSS3.1 Base: -

CVSS3.1 Temporal: -

CVSS Environment: -

Asset Group: -

Collateral Damage Potential: -

Target Distribution: -

Confidentiality Requirement: -

Integrity Requirement: -

Availability Requirement: -

Times Detected: 5

Last Fixed: N/A

THREAT:
The host is running CentOS 5.x.
CentOS ended support for 5 on March 31, 2017 and provides no further support for this operating system.

► 4 CentOS Security Update for kernel (CESA-2017-0323)

CVSS: 5.9 CVSS3.1: 7.2 Active

► 3 Deprecated SSH Cryptographic Settings

port 22/tcp CVSS: 4.7 CVSS3.1: 5.3 Active

Issues Addressed

- We fixed an issue where the user could not activate PCI Account. The user can now successfully activate their PCI accounts.
- We fixed an issue where user was not able to run compliance interactive reports in AGMS enabled account which does not have network support.
- Now users in SCA only subscriptions can schedule scans on asset groups that contain only DNS names.
- We fixed an issue where the incorrect first found date was showing for the asset in the ASR filter “First found within 7 days.”
- We fixed an issue where the “Do not show tutorial” button was not functioning correctly; it showed available tutorials for the different tabs despite selecting the “Do not show tutorial” option.
- We fixed an issue so Information Gathered QIDs (which are detected in Agent scan, but not detected in scanner authenticated scan) are correctly synced with valid result data for the agent merge scenario.
- We fixed an issue where users were not able to view posture data for some assets they were assigned based on tags because the tag hierarchy was not fully being considered. Now users should be able to view posture data for assets based on any level of tag hierarchy.
- Now when you delete an asset group, the Conflict Report will include a list of compliance policies affected by the change and activity logs are also updated to list policies.
- We fixed an issue where an error pop-up was displayed after a certain percentage was reached while downloading a template-based scan report in PDF format.
- We fixed an issue where unexpected characters appeared in the API output of scanner appliance list when include_cloud_info=1 was included in the API request.
- We fixed an issue where the Update action for Unix authentication record using the API returned an error when multiple record IDs were specified in the API request.
- We fixed an issue where the Authentication Details page was not being properly updated in cases where “Tag Support for Authentication Records” is enabled and the authentication records map to EC2 hosts.
- The Ignore Vulnerability API failed to ignore vulnerabilities if the vulnerability was detected on multiple ports. We have now fixed this issue so that vulnerability is ignored despite being detected on multiple ports.
- The report option “Exclude QIDs not exploitable due to configuration” is now working as expected for Scorecard Reports.
- We fixed the issue where the report took a long time in the case of host-based reports in CSV/XML format.
- Before this release, when the scanner appliance was moved from one network to another network and though the scheduled scan failed, the activity was still getting recorded as successful. As a result, the “Scan Launch Successful” message was shown. With this release, this issue has been fixed, and now a message “Scan launch failed.255” is shown that provides the correct scan status along with the error code. Also, if the user has opted to receive the email notification if the launch is skipped, the email notification is sent to the user.

- Before this release, for the Asset Group Management Service (AGMS) enabled account, when you deleted an asset group, the name of the asset group and the asset Id was not shown in the message. With this release, we have fixed this issue. The message now includes the name of the asset group and asset id in the “AssetGroupId (Asset Group Name)” format.
- We fixed an issue where the user was not able to remove an FQDN from a VM scheduled scan to replace it with an IP.