Qualys OpenSSL Service Playbook

December 02, 2022

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Qualys OpenSSL Service Playbook

Since the OpenSSL vulnerability was first discovered, the Qualys Research Team has analyzed the threat and updated the Qualys Cloud Platform to help customers respond quickly. We recognize that the scope of the challenge is significant for many organizations, as it involves core open-source libraries in their environment. Two vulnerabilities need to be addressed: CVE-2022-3602 (remote code execution) and CVE-2022-3786 (denial of service).

OpenSSL project team rates the severity of the vulnerability as HIGH, which means this vulnerability affects common configurations and is also likely to be exploitable.

What versions are impacted?

OpenSSL versions 3.0.0 - 3.0.6 are affected by these two vulnerabilities. OpenSSL 1.1.1, which is commonly deployed, is not vulnerable. OpenSSL 3.0 applications that verify X.509 certificates received from untrusted sources should be considered vulnerable.

What can you do to protect yourself?

Qualys recommends that organizations take a prioritized, layered approach to remediate and eliminate this vulnerability wherever it lives. Read more about OpenSSL in our blog:

https://blog.qualys.com/vulnerabilities-threat-research/2022/10/31/qualys-research-alert-prepare-for-a-critical-vulnerability-in-openssl-3-0

Refer to Qualys documentation and blogs to know more and set up and configure Qualys apps, as required. We encourage OpenSSL 3.0.0 - 3.0.6 users to upgrade to 3.0.7 as soon as possible.

What are the immediate actions you need to take?

The primary objective is to determine the existence of any vulnerabilities. To begin this process, Qualys recommends that all organizations scan their external attack surface (public-facing websites and applications) to identify potential vulnerabilities by simulating the attack using the Qualys Web Application Scanning module.

Recommended Steps:

1. Scan your external attack surface using Qualys Web Application Scanner (WAS)
2. Find vulnerabilities and prioritize using Qualys Cybersecurity Asset Management (CSAM)
3. Discover vulnerable OpenSSL packages using Qualys Vulnerability Management Detection and Response (VMDR)
4. Discover Vulnerable Container Images Using Qualys Container Security (CS)
5. Initiate Endpoint Response Actions via Customer Assessment and Remediation (CAR)

Scan Your External Attack Surface

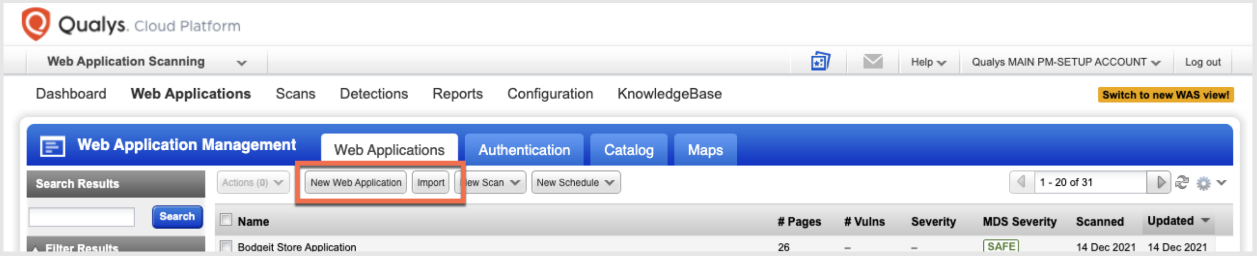
Qualys Web Application Scanning (WAS)

For details on Qualys WAS OpenSSL detection, please refer to our blog.

Use our Web Application Scanning (WAS) to find web applications and APIs vulnerable to OpenSSL (CVE-2022-3786 and CVE-2022-3602). WAS injects JNDI payloads into certain request headers and application-specific endpoints. It uses Out-Of-Band (OOB) detection methods where vulnerable instances will make a callback DNS query that will trigger the Qualys Periscope detection mechanism.

Step 1 - Identify Web Applications to Scan

You can either add a new application or import an existing one by navigating to the Web Applications > Web Applications tab. For detailed steps, refer to Adding Web Applications.



Name	# Pages	# Vulns	Severity	MDS Severity	Scanned	Updated
Bodgeit Store Application	26	–	–	SAFE	14 Dec 2021	14 Dec 2021

Refer to the following docs to get started with WAS
WAS Videos | WAS Getting Started Guide | WAS Online Help

Step 2 - Use the OpenSSL Option profile to scan

Navigate to the Configuration > Options Profile tab and click Import Profile to import the OpenSSL Options scanning option profile.

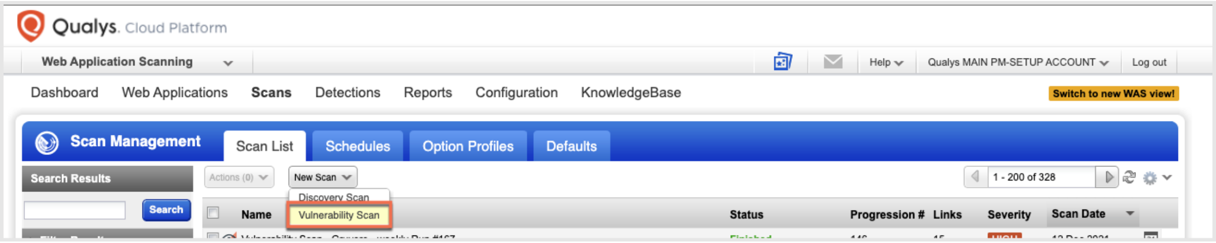
By using this OpenSSL option profile, you can expedite testing your web applications for QIDs 38879. This approach can accelerate web application scanning and identify vulnerable OpenSSL versions.

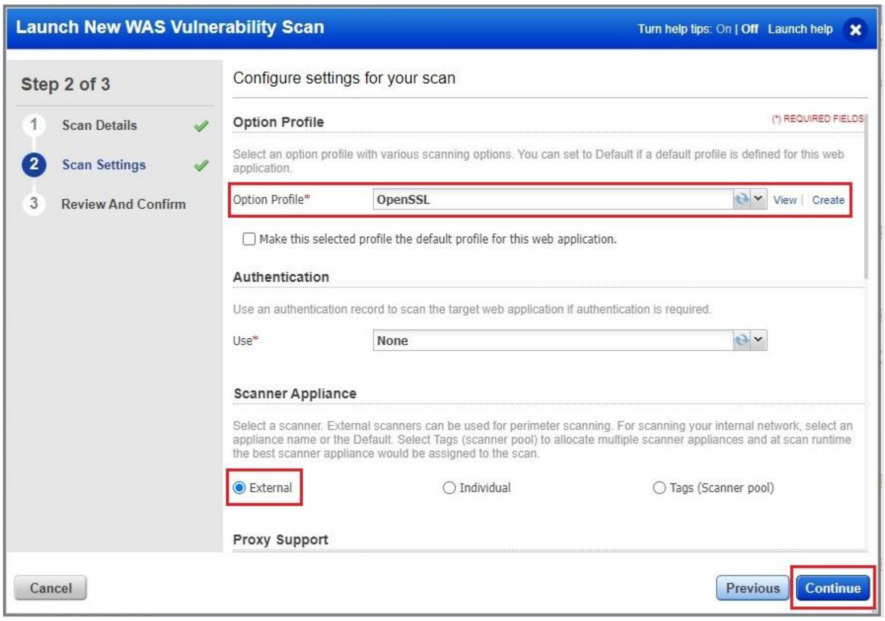
QID currently detects vulnerable OpenSSL installations on Windows, but Linux support is coming soon.

Refer to Manage Options Profile

Step 3 – Launch a Web Application Scan

Navigate to the Scan tab, and from Scan List, select Vulnerability Scan. Select the OpenSSL Options scanning option profile and then select the external scanner.





Configure settings for your scan

Option Profile

(*) REQUIRED FIELDS

Select an option profile with various scanning options. You can set to Default if a default profile is defined for this web application.

Option Profile* OpenSSL

□ Make this selected profile the default profile for this web application.

Authentication

Use an authentication record to scan the target web application if authentication is required.

Use* None

Scanner Appliance

Select a scanner. External scanners can be used for perimeter scanning. For scanning your internal network, select an appliance name or the Default. Select Tags (scanner pool) to allocate multiple scanner appliances and at scan runtime the best scanner appliance would be assigned to the scan.

● External ○ Individual ○ Tags (Scanner pool)

Proxy Support

That's it! Click Continue to launch your scan. Upon completion of the scan, reports can be generated that outline any OpenSSL vulnerabilities.

Find Vulnerabilities and Prioritize

This vulnerability poses a significant detection challenge. Detecting vulnerabilities in core open-source libraries using a vulnerable version of OpenSSL is a multi-layered approach Qualys offers its customers.

Qualys Cybersecurity Asset Management (CSAM)

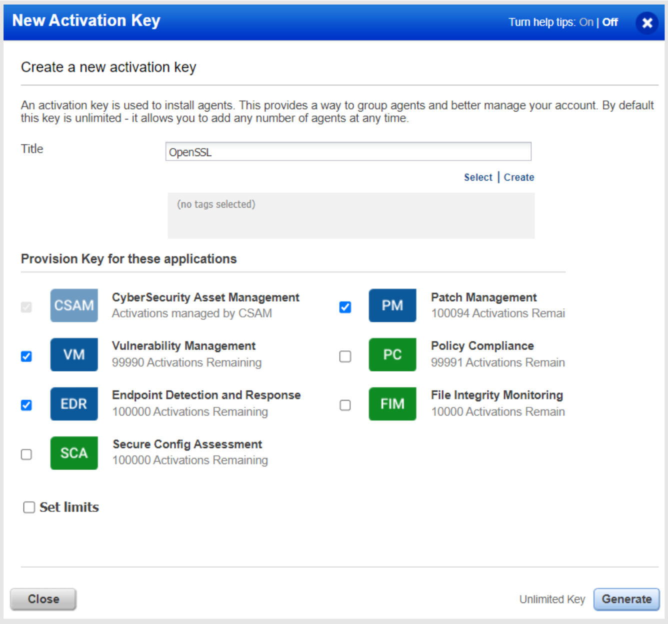
Secure your infrastructure by determining which components are vulnerable to OpenSSL vulnerabilities. By identifying and updating components, you can reduce the attack surface of your infrastructure.

Step 1 - Deploy and Setup Cloud Agent

Build your inventory using cloud agents. To continuously discover your IT assets in real-time, you can deploy agents in private clouds, public clouds, on-premises, and on endpoints.

Install Qualys Cloud Agents | Cloud Agent Getting Started Guide | Cloud Agent Onboarding Videos

Create an OpenSSL activation key in Cloud Agent. Select VM, EDR, and Patch Management, and follow the wizard to install the agents for all endpoints you want to protect.



New Activation Key

Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title: OpenSSL

(no tags selected)

Provision Key for these applications

- ☑ CSAM — CyberSecurity Asset Management — Activations managed by CSAM
- ☑ PM — Patch Management — 100094 Activations Remai
- ☑ VM — Vulnerability Management — 99990 Activations Remaining
- □ PC — Policy Compliance — 99991 Activations Remain
- ☑ EDR — Endpoint Detection and Response — 100000 Activations Remaining
- □ FIM — File Integrity Monitoring — 10000 Activations Remain
- □ SCA — Secure Config Assessment — 100000 Activations Remaining

□ Set limits

Unlimited Key

Once the agent is installed, it collects and inventories all vulnerabilities and assets. It is then possible to identify and mitigate OpenSSL vulnerabilities.

Step 2 - Detect at-risk Assets & Applications

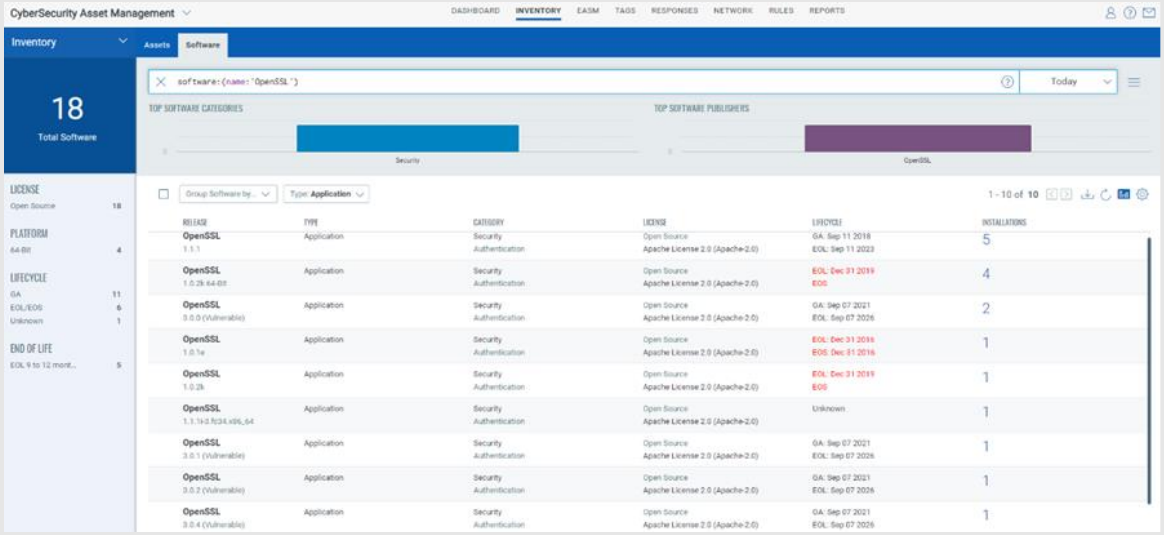
CSAM enriches your asset inventory with relevant, in-context information to detect at-risk assets and applications. You can identify and set alerts for assets that have OpenSSL vulnerabilities.

Refer to the following documentation to get started with CSAM

CSAM Quick Start Guide | CSAM Onboarding Videos | CSAM Online Help

CSAM makes it easy to identify assets with vulnerable versions of OpenSSL. To identify such assets, use the following QQL query.

Query: software:(name:OpenSSL and version>=3.0 and version< 3.0.7)



software:(name:"OpenSSL")

18 Total Software

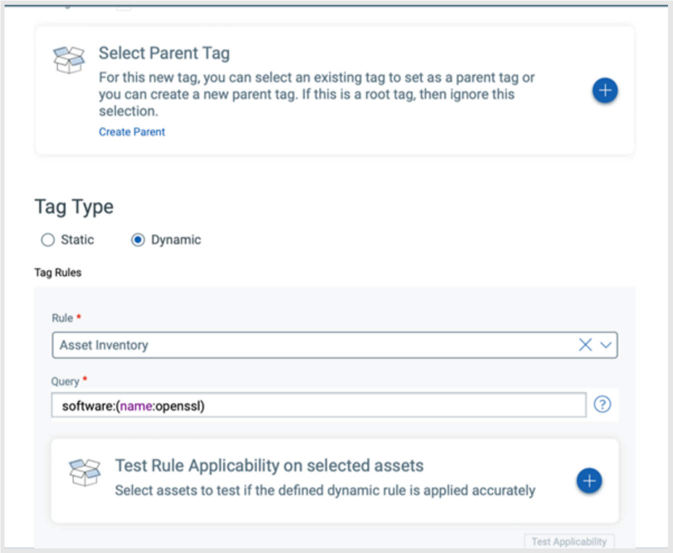
LICENSE: Open Source 18
PLATFORM: 64-Bit 4
LIFECYCLE: GA 11; EOL/EOS 6; Unknown 1
END OF LIFE: EOL 9 to 12 mont... 5

Type: Application

1 - 10 of 10

RELEASE	TYPE	CATEGORY	LICENSE	LIFECYCLE	INSTALLATIONS
OpenSSL 1.1.1	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2.0)	GA: Sep 11 2018 EOL: Sep 11 2023	5
OpenSSL 1.0.2k 64-Bit	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2.0)	EOL: Dec 31 2019 EOS	4
OpenSSL 3.0.0 (Vulnerable)	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2.0)	GA: Sep 07 2021 EOL: Sep 07 2026	2
OpenSSL 1.0.1e	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2.0)	EOL: Dec 31 2016 EOS: Dec 31 2016	1
OpenSSL 1.0.2k	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2.0)	EOL: Dec 31 2019 EOS	1
OpenSSL 1.1.1k-3.fc34.x86_64	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2.0)	Unknown	1
OpenSSL 3.0.1 (Vulnerable)	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2.0)	GA: Sep 07 2021 EOL: Sep 07 2026	1
OpenSSL 3.0.2 (Vulnerable)	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2.0)	GA: Sep 07 2021 EOL: Sep 07 2026	1
OpenSSL 3.0.4 (Vulnerable)	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2.0)	GA: Sep 07 2021 EOL: Sep 07 2026	1

A newly published rule in Qualys CSAM lists and tags all applications that use the vulnerable OpenSSL component. Run a scan with the OpenSSL detection rule enabled to identify vulnerable applications.



Select Parent Tag

For this new tag, you can select an existing tag to set as a parent tag or you can create a new parent tag. If this is a root tag, then ignore this selection.

Create Parent

Tag Type

○ Static ● Dynamic

Tag Rules

Rule *

Asset Inventory

Query *

software:(name:openssl)

Test Rule Applicability on selected assets

Select assets to test if the defined dynamic rule is applied accurately

Test Applicability

Click CSAM > Rules, select the rule "Apps with OpenSSL (potentially vulnerable)," then click Actions and enable the rule. You can now view and categorize assets with the OpenSSL component in the Inventory tab.

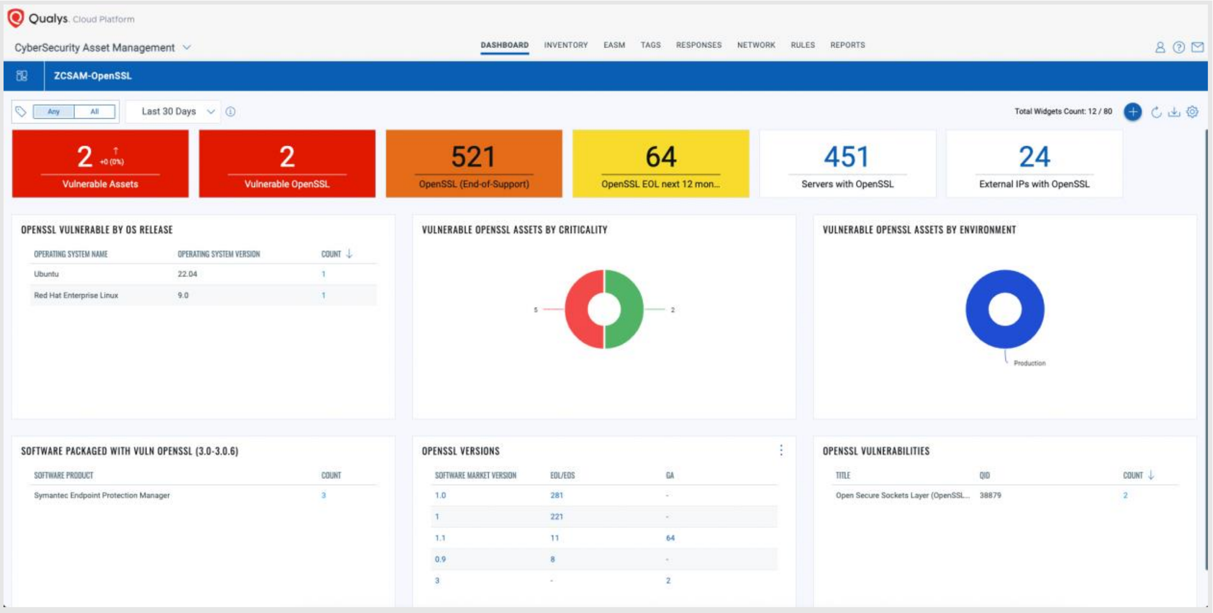
Enrich the Inventory
To run more efficient inventory queries for suspected asset vulnerabilities, the Qualys Research Team has enhanced the inventory data collected by CSAM. We can flag applications recognized as vulnerable to the OpenSSL exploit using GitHub. You can start your queries with your externally facing assets marked as vulnerable. CSAM integration with your CMDB allows you to focus on business-critical applications first, allowing you to prioritize them.

Step 3 – Visualize OpenSSL Exposure

An application that uses a vulnerable version of OpenSSL can be considered potentially vulnerable. With our dashboards, you can quickly identify vulnerable hosts and software. The widgets in the dashboard display vulnerable hosts, applications with vulnerable OpenSSL versions, and, most importantly, vulnerable hosts visible on the Internet.

Dedicated widgets such as ‘External Attack Surface’ populate all vulnerable hosts visible on Shodan and are low-hanging opportunities for attackers. These widgets also list workloads hosted on shared cloud infrastructure with public IP addresses.

You can read more about Qualys integration with Shodan here.



2 +0 (0%) Vulnerable Assets | 2 Vulnerable OpenSSL | 521 OpenSSL (End-of-Support) | 64 OpenSSL EOL next 12 mon... | 451 Servers with OpenSSL | 24 External IPs with OpenSSL

OPENSSL VULNERABLE BY OS RELEASE

OPERATING SYSTEM NAME	OPERATING SYSTEM VERSION	COUNT ↓
Ubuntu	22.04	1
Red Hat Enterprise Linux	9.0	1

VULNERABLE OPENSSL ASSETS BY CRITICALITY

VULNERABLE OPENSSL ASSETS BY ENVIRONMENT

SOFTWARE PACKAGED WITH VULN OPENSSL (3.0-3.0.6)

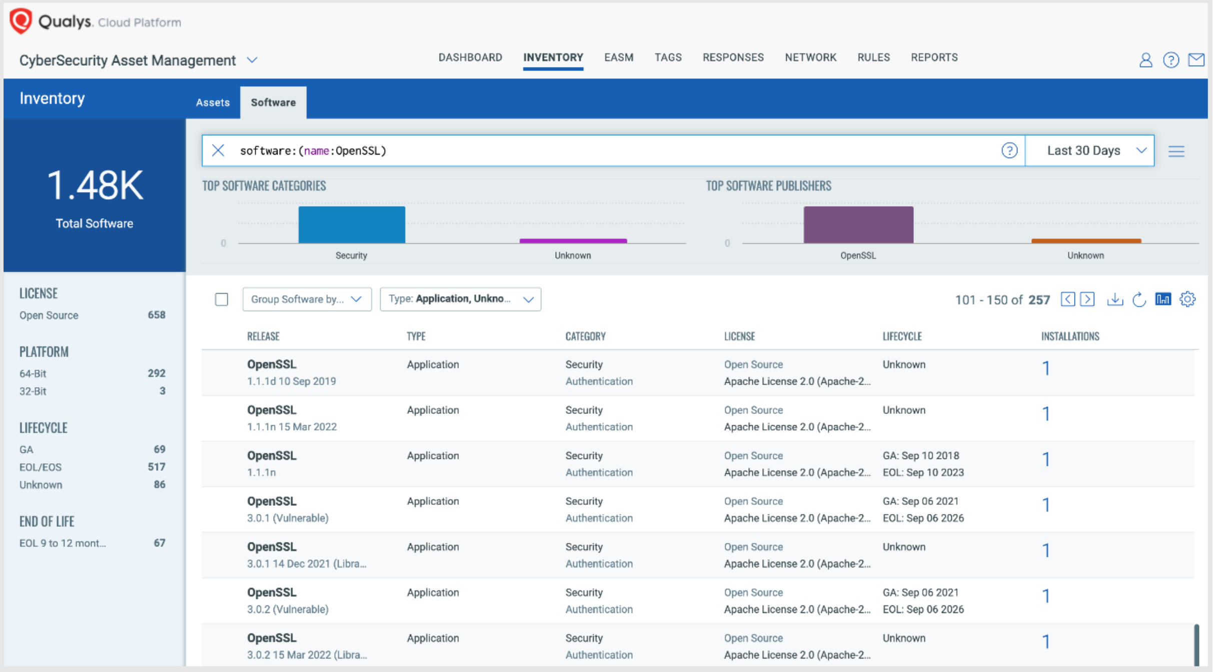
SOFTWARE PRODUCT	COUNT
Symantec Endpoint Protection Manager	3

OPENSSL VERSIONS

SOFTWARE MARKET VERSION	EOL/EOS	GA
1.0	281	-
1	221	-
1.1	11	64
0.9	8	-
3	-	2

OPENSSL VULNERABILITIES

TITLE	QID	COUNT ↓
Open Secure Sockets Layer (OpenSSL...	38879	2



software:(name:OpenSSL)

1.48K Total Software

LICENSE	
Open Source	658
PLATFORM	
64-Bit	292
32-Bit	3
LIFECYCLE	
GA	69
EOL/EOS	517
Unknown	86
END OF LIFE	
EOL 9 to 12 mont...	67

RELEASE	TYPE	CATEGORY	LICENSE	LIFECYCLE	INSTALLATIONS
OpenSSL 1.1.1d 10 Sep 2019	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2...	Unknown	1
OpenSSL 1.1.1n 15 Mar 2022	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2...	Unknown	1
OpenSSL 1.1.1n	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2...	GA: Sep 10 2018 EOL: Sep 10 2023	1
OpenSSL 3.0.1 (Vulnerable)	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2...	GA: Sep 06 2021 EOL: Sep 06 2026	1
OpenSSL 3.0.1 14 Dec 2021 (Libra...	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2...	Unknown	1
OpenSSL 3.0.2 (Vulnerable)	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2...	GA: Sep 06 2021 EOL: Sep 06 2026	1
OpenSSL 3.0.2 15 Mar 2022 (Libra...	Application	Security Authentication	Open Source Apache License 2.0 (Apache-2...	Unknown	1

Refer to the following Unified Dashboard online help on building and using dashboards.

Qualys Vulnerability Management Detection and Response (VMDR)

With your inventory in place, you can use VMDR to assess, prioritize, and remediate OpenSSL vulnerabilities.

Through VMDR, you can automatically discover and prioritize the specially researched OpenSSL vulnerabilities, and with threat feeds, you can identify high-profile vulnerabilities to which your assets might be exposed.

Refer to the following documentation to get started with VMDR

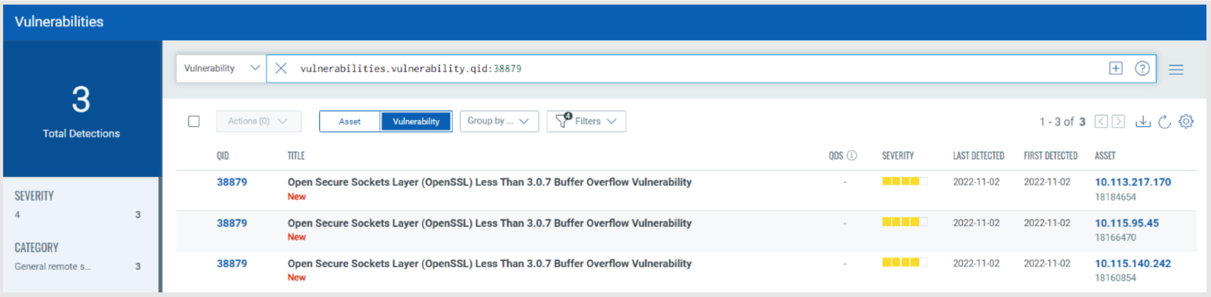
VMDR Onboarding Videos | VMDR Getting Started Guide | VMDR Online Help

Step 1 – Detect OpenSSL vulnerability

There are two ways to detect OpenSSL vulnerability.

1) In the Vulnerabilities view, using the QQL query, you can view all your impacted hosts for OpenSSL vulnerability. Search for vulnerabilities using the following query in the VMDR > Vulnerabilities tab:

   vulnerabilities.vulnerability.qid:[`38879`]



```
vulnerabilities.vulnerability.qid:38879
```

3 Total Detections

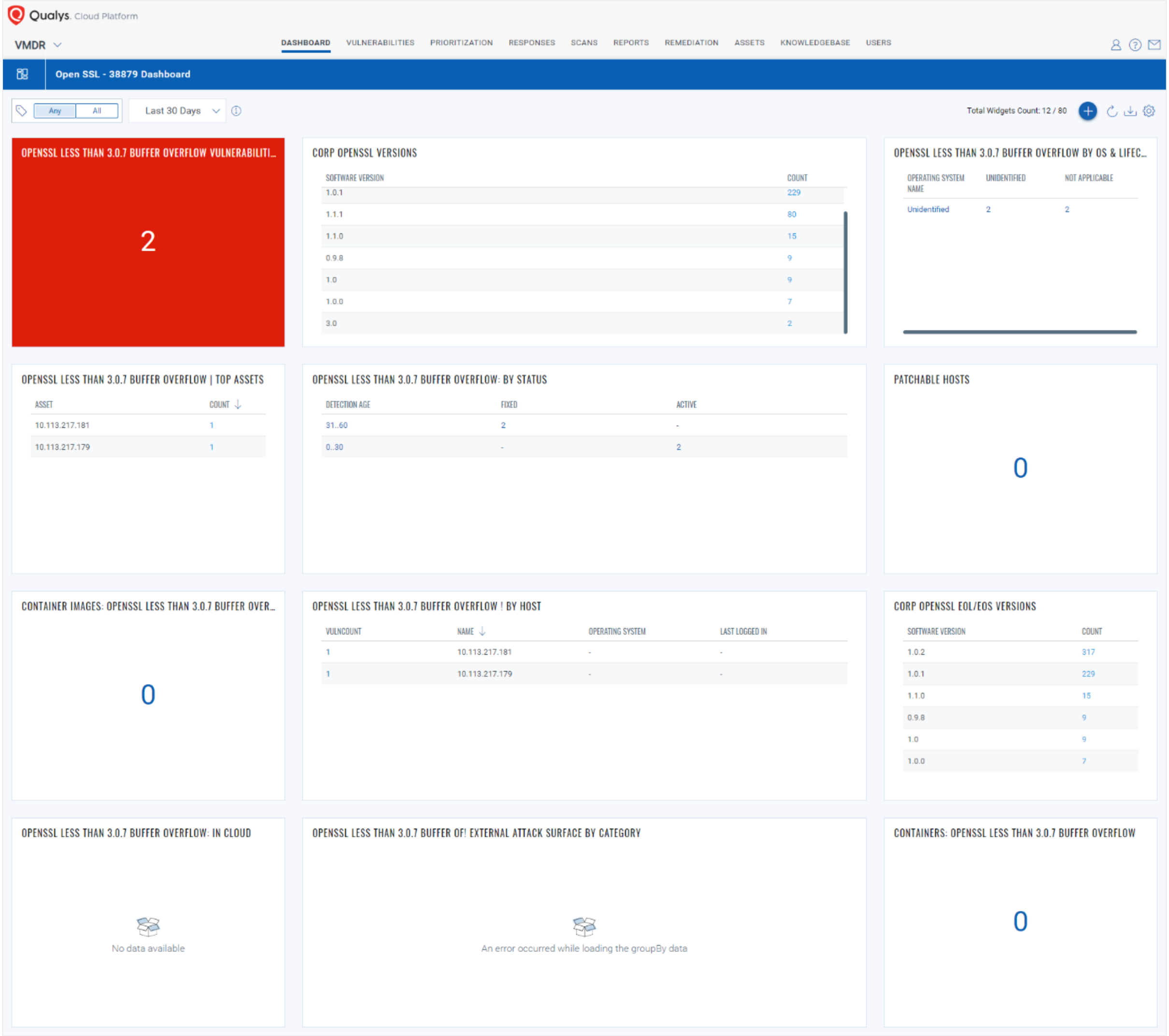
SEVERITY 4 3

CATEGORY General remote s... 3

QID	TITLE	QDS	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
38879	Open Secure Sockets Layer (OpenSSL) Less Than 3.0.7 Buffer Overflow Vulnerability New	-	🟨🟨🟨🟨	2022-11-02	2022-11-02	10.113.217.170 18184654
38879	Open Secure Sockets Layer (OpenSSL) Less Than 3.0.7 Buffer Overflow Vulnerability New	-	🟨🟨🟨🟨	2022-11-02	2022-11-02	10.115.95.45 18166470
38879	Open Secure Sockets Layer (OpenSSL) Less Than 3.0.7 Buffer Overflow Vulnerability New	-	🟨🟨🟨🟨	2022-11-02	2022-11-02	10.115.140.242 18160854

2) Prioritize vulnerabilities based on Assets. Using VMDR, the OpenSSL vulnerabilities can be prioritized based on assets using the following:
   - Asset Risk Score (ARS): an intelligence-driven vulnerability severity scoring
   - Asset Criticality Score (ASC): display the asset criticality score for each asset
   - Internet facing using EASM: gives you comprehensive visibility to monitor the external-facing organization's infrastructure network to discover the vulnerable systems, target attacks, and campaigns.

Step 2 – Generate Prioritization Report



Open SSL - 38879 Dashboard

Total Widgets Count: 12 / 80

OPENSSL LESS THAN 3.0.7 BUFFER OVERFLOW VULNERABILITI...

2

CORP OPENSSL VERSIONS

SOFTWARE VERSION	COUNT
1.0.1	229
1.1.1	80
1.1.0	15
0.9.8	9
1.0	9
1.0.0	7
3.0	2

OPENSSL LESS THAN 3.0.7 BUFFER OVERFLOW BY OS & LIFEC...

OPERATING SYSTEM NAME	UNIDENTIFIED	NOT APPLICABLE
Unidentified	2	2

OPENSSL LESS THAN 3.0.7 BUFFER OVERFLOW | TOP ASSETS

ASSET	COUNT ↓
10.113.217.181	1
10.113.217.179	1

OPENSSL LESS THAN 3.0.7 BUFFER OVERFLOW: BY STATUS

DETECTION AGE	FIXED	ACTIVE
31..60	2	-
0..30	-	2

PATCHABLE HOSTS

0

CONTAINER IMAGES: OPENSSL LESS THAN 3.0.7 BUFFER OVER...

0

OPENSSL LESS THAN 3.0.7 BUFFER OVERFLOW ! BY HOST

VULNCOUNT	NAME ↓	OPERATING SYSTEM	LAST LOGGED IN
1	10.113.217.181	-	-
1	10.113.217.179	-	-

CORP OPENSSL EOL/EOS VERSIONS

SOFTWARE VERSION	COUNT
1.0.2	317
1.0.1	229
1.1.0	15
0.9.8	9
1.0	9
1.0.0	7

OPENSSL LESS THAN 3.0.7 BUFFER OVERFLOW: IN CLOUD

No data available

OPENSSL LESS THAN 3.0.7 BUFFER OF! EXTERNAL ATTACK SURFACE BY CATEGORY

An error occurred while loading the groupBy data

CONTAINERS: OPENSSL LESS THAN 3.0.7 BUFFER OVERFLOW

0

Qualys Container Security (CS)

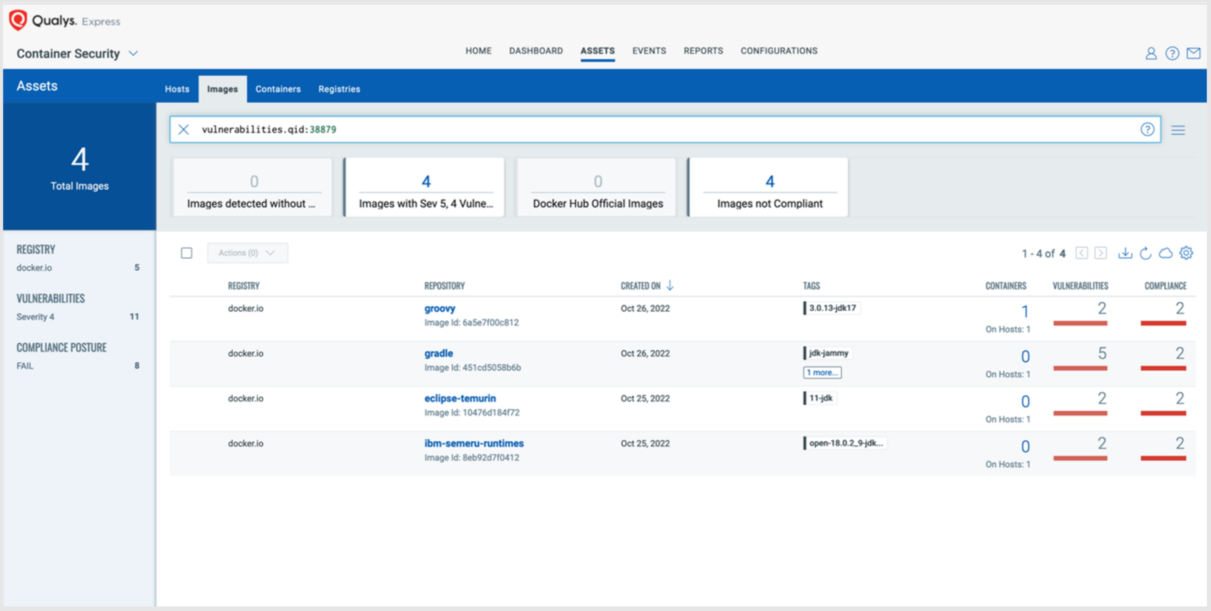
As containers are common in many environments, scanning for the OpenSSL vulnerability in your containers is a critical next step. Container Security offers multiple methods to help you detect OpenSSL vulnerabilities for running containers and container images in your container environment. Qualys Container Security (CS) can detect vulnerable versions of OpenSSL 3.0 through 3.0.6 with QID 38879.

Step 1 - Scan Containers

Navigate to Container Security > Assets > Containers and search using the following query:

vulnerabilities.qid: `38879`

Click the resulting vulnerable containers and go to the “Vulnerabilities” tab to learn more.



```
vulnerabilities.qid:38879
```

REGISTRY	REPOSITORY	CREATED ON	TAGS	CONTAINERS	VULNERABILITIES	COMPLIANCE
docker.io	groovy Image Id: 6a5e7f00c812	Oct 26, 2022	3.0.13-jdk17	1 On Hosts: 1	2	2
docker.io	gradle Image Id: 451cd5058b6b	Oct 26, 2022	jdk-jammy 1 more...	0 On Hosts: 1	5	2
docker.io	eclipse-temurin Image Id: 10476d184f72	Oct 25, 2022	11-jdk	0 On Hosts: 1	2	2
docker.io	ibm-semeru-runtimes Image Id: 8eb92d7f0412	Oct 25, 2022	open-18.0.2_9-jdk...	0 On Hosts: 1	2	2

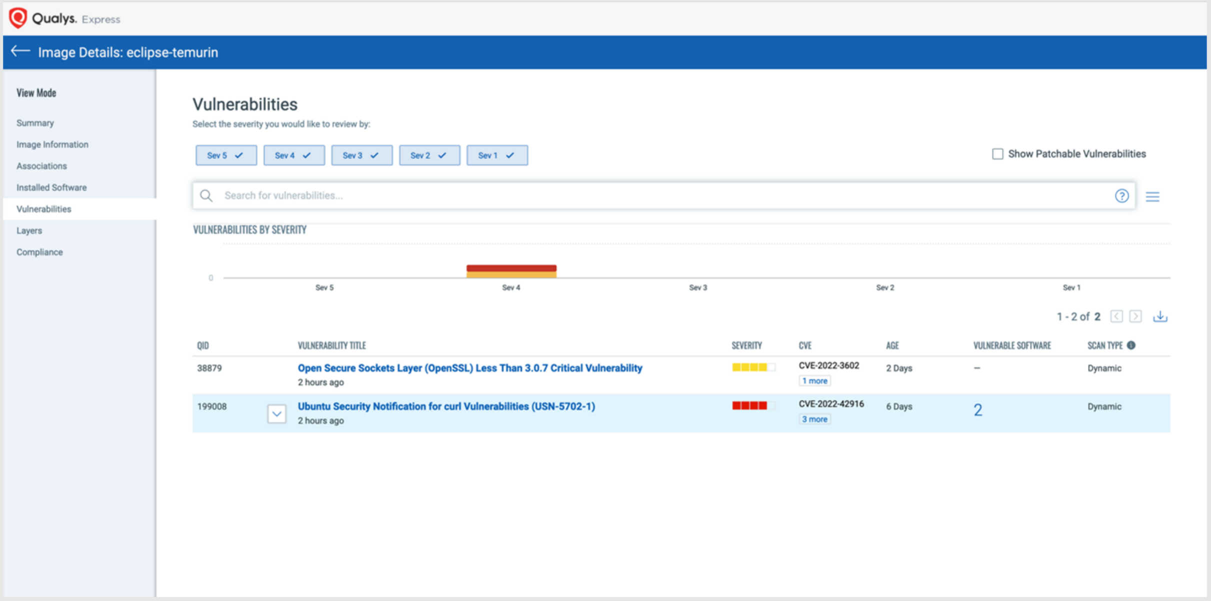
Step 2 – Scan Images

Qualys also recommends scanning your images. Running scans on images will mitigate vulnerabilities when the image is instantiated into a container later.

To scan Images, navigate to Container Security > Assets > Images and search using the following query:

vulnerabilities.qid: `38879`

Click the resulting vulnerable containers and go to the “Vulnerabilities” tab to learn more.



QID	VULNERABILITY TITLE	SEVERITY	CVE	AGE	VULNERABLE SOFTWARE	SCAN TYPE
38879	Open Secure Sockets Layer (OpenSSL) Less Than 3.0.7 Critical Vulnerability 2 hours ago	🟨🟨🟨🟨	CVE-2022-3602 1 more	2 Days	–	Dynamic
199008	Ubuntu Security Notification for curl Vulnerabilities (USN-5702-1) 2 hours ago	🟥🟥🟥🟥	CVE-2022-42916 3 more	6 Days	2	Dynamic

This in-depth container image scan can be triggered in three stages of your container’s image lifecycle: during the build process, as the image is uploaded to the register, and before the image is deployed to production.

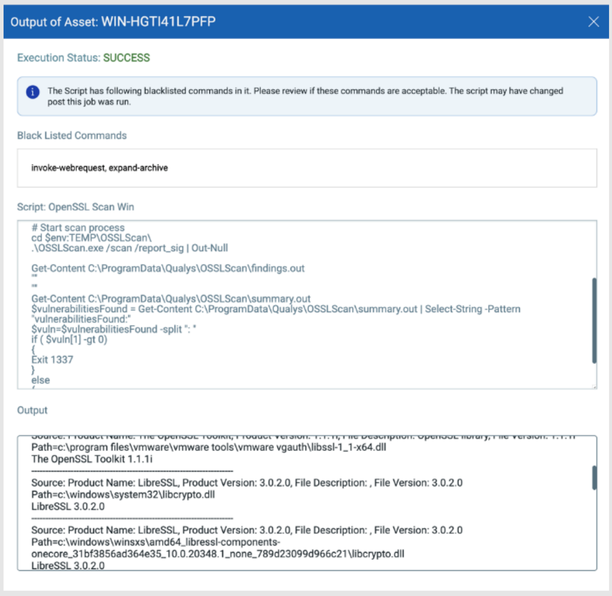
Refer to the following documentation to get started with Container Security

Container Security Videos | Container Security User Guide | Container Security Online Help

Remediate

Customer Assessment and Remediation (CAR)

Out-of-Band Detection for OpenSSL can be run on assets/asset tags required by customers. Time is a critical factor in zero-day situations. Organizations are vulnerable to security risks if detection and remediation are delayed. Qualys Custom Assessment and Remediation (CAR) allows security practitioners to collect data quickly, execute custom scripts, and initiate action responses on endpoints. This can reduce MTTRs for zero-day attacks and other threats by 50% or more.



Output of Asset: WIN-HGTI41L7PFP

Execution Status: SUCCESS

The Script has following blacklisted commands in it. Please review if these commands are acceptable. The script may have changed post this job was run.

Black Listed Commands

invoke-webrequest, expand-archive

Script: OpenSSL Scan Win

```
# Start scan process
cd $env:TEMP\OSSLScan\
.\OSSLScan.exe /scan /report_sig | Out-Null

Get-Content C:\ProgramData\Qualys\OSSLScan\findings.out
""
""
Get-Content C:\ProgramData\Qualys\OSSLScan\summary.out
$vulnerabilitiesFound = Get-Content C:\ProgramData\Qualys\OSSLScan\summary.out | Select-String -Pattern
"vulnerabilitiesFound:"
$vuln=$vulnerabilitiesFound -split ": "
if ( $vuln[1] -gt 0)
{
Exit 1337
}
else
```

Output

```
Source: Product Name: The OpenSSL Toolkit, Product Version: 1.1.1i, File Description: OpenSSL library, File Version: 1.1.1i
Path=c:\program files\vmware\vmware tools\vmware vgauth\libssl-1_1-x64.dll
The OpenSSL Toolkit 1.1.1i
-------------------------------------------------------------------
Source: Product Name: LibreSSL, Product Version: 3.0.2.0, File Description: , File Version: 3.0.2.0
Path=c:\windows\system32\libcrypto.dll
LibreSSL 3.0.2.0
-------------------------------------------------------------------
Source: Product Name: LibreSSL, Product Version: 3.0.2.0, File Description: , File Version: 3.0.2.0
Path=c:\windows\winsxs\amd64_libressl-components-
onecore_31bf3856ad364e35_10.0.20348.1_none_789d23099d966c21\libcrypto.dll
LibreSSL 3.0.2.0
```

Qualys CAR customers can use the Out-of-Band Detection utility for Windows to scan assets/asset tags for OpenSSL vulnerabilities. This utility scans the entire hard drive(s), including archives (and nested JARs) for OpenSSL libraries that indicate the application contains OpenSSL libraries. You can view the results of the utility on the console.

Refer to the following documentation to get started with CAR

CAR Getting Started Guide | CAR Online Help | Working with Scripts

Script Library for Custom Assessment and Remediation

Qualys provides a library of script templates that can be used in various real-life scenarios. The library is regularly updated with scripts for detecting and mitigating zero-day vulnerabilities like Log4Shell, Text4Shell, ProxyNotShell, and OpenSSL.

Take advantage of Qualys CAR Script Library's best-in-class content to solve your use cases. You can use the library's use-case-based scripts to reduce the overall MTTR of your incident response program. The scripts can also serve as templates that can be modified based on business needs.