

# Vulnerability Scans

FortiSIEM 6.3.3



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



01/26/2022

FortiSIEM 6.3.3 Vulnerability Scans

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Running Vulnerability Scans against FortiSIEM</b>	<b>5</b>
Qualys Configuration	5
Step 1: Configure Scan Profile	5
Step 2: Setup Host Authentication	5
Step 3: Add Host IPs to Scan	5
Step 4: Launch Vulnerability Scan	5
Nessus Configuration	6
Step 1: Configure Scan and Host IP	6
Step 2: Setup Host Authentication	6
Step 3: Launch Vulnerability Scan	6
Rapid7 Configuration	6
Step 1: Install Rapid7 Insight Agent on FortiSIEM	6
Step 2: Validate FortiSIEM Vulnerability Scan Results	7
<b>Validating Vulnerability Scan Results</b>	<b>8</b>
Find the CVE Information in the RedHat Database	8
Validate Redhat Fixed Vulnerabilities in FortiSIEM	9
<b>Mitigating Found Vulnerabilities</b>	<b>12</b>

# Change Log

Date	Change Description
04/17/2018	Initial version of the document.
03/25/2019	Revision 1: Removed "FortiSIEM Configuration" section.
08/19/2019	Revision 2: Updated the location of the image download site.
11/20/2019	Vulnerability Scans released for 5.2.6.
02/11/2020	Revision 3: Added the section <a href="#">Validating Vulnerability Scan Results</a> .
03/30/2020	Revision 4: Release for 5.3.0. Added section for configuring Rapid7 for vulnerability scans.
03/23/2021	Revision 5: Release for 6.2.0.
07/06/2021	Revision 6: Release for 6.3.0.
08/26/2021	Revision 7: Release for 6.3.1.
10/15/2021	Revision 8: Release for 6.3.2.
12/22/2021	Revision 9: Release for 6.3.3.

# Running Vulnerability Scans against FortiSIEM

This document provides information about the configurations for running vulnerability scans against FortiSIEM.

- [Qualys Configuration](#)
- [Nessus Configuration](#)
- [Rapid7 Configuration](#)

## Qualys Configuration

Logon to Qualys Vulnerability Management and follow the steps below to run a Vulnerability scan:

### Step 1: Configure Scan Profile

1. Go to **Scans > Option Profiles** and click **New > PCI Option Profile**.
2. On the 'New PCI Option Profile' window, click the **Scan** tab.
3. Select 'Unix/Cisco' Authentication.
4. Click **Save**.

### Step 2: Setup Host Authentication

1. Go to **Scans > Authentication** and click **New > Unix Record**.
2. On the 'New Unix Record' pop-up, add the login credentials.
3. Click the **IPs** tab and enter the Host IPs and click **Create**.

### Step 3: Add Host IPs to Scan

1. Go to **Assets > Host Assets**.
2. Click **New > IP Tracked Hosts**.
3. Enter the new **Host IPs** and click **Add**.

### Step 4: Launch Vulnerability Scan

1. Go to **Scans > Scans** tab.
2. Click **New > Scans** and select the **Option Profile** added in [step #2](#).
3. Select Host IPs that added in [step #2](#).
4. Click **Launch** to start the scan.

## Nessus Configuration

Logon to Tenable Nessus Scanner UI and follow the steps below to run a Vulnerability scan:

### Step 1: Configure Scan and Host IP

1. Go to **Scans** and click **New Scan > Advanced Network Scan**.
2. Under **Settings** tab, enter the information about the new scan including the FortiSIEM Host IP under **Targets**.
3. Click **Save**.

### Step 2: Setup Host Authentication

1. Go to **Scans** and select the Scan added in [Step #1](#).
2. Click **Configure**.
3. Under the **Credentials** tab, click **SSH** and enter the FortiSIEM credentials.
4. Click **Save**.

### Step 3: Launch Vulnerability Scan

1. Go to **Scans** and select the Scan from [Step #1](#).
2. Click the **Launch** icon to start the scan.

## Rapid7 Configuration

Logon to Rapid7 insightVM (Advanced Vulnerability Management Analytics and Reporting) and follow these steps to run a Vulnerability scan:

### Step 1: Install Rapid7 Insight Agent on FortiSIEM

1. Logon to Rapid7 insightVM (Advanced Vulnerability Management Analytics and Reporting).
2. Go to the **Agent Management** page, then select **Add New > Agent**.
3. Download the Rapid7 Linux Agent and copy it to FortiSIEM.
4. SSH to FortiSIEM and install Rapid7 Insight Agent with Token, for example:  

```
sudo ./agent_installer.sh install_start --token us:bf870020-ef0b-41de-9c9e-da45237c214d
```

## Step 2: Validate FortiSIEM Vulnerability Scan Results

1. In the Rapid7 insightVM UI, go to the **Agent Management** page and check the recently installed Agent.
2. Go to the insightVM default dashboard.
3. In the **Newly discovered Assets** gadget, click **Assets**.
4. In the **Assets** list, click the FortiSIEM hostname.
5. On the **Asset Details** page, validate the list of vulnerabilities.

# Validating Vulnerability Scan Results

The following sections describe how to validate vulnerability scan results:

- [Find the CVE Information in the RedHat Database](#)
- [Validate Redhat Fixed Vulnerabilities in FortiSIEM](#)

## Find the CVE Information in the RedHat Database

1. Log in to the Vulnerability scanner.
2. Run a Vulnerability scan against FortiSIEM. See [Running Vulnerability Scans against FortiSIEM](#).
3. In the Vulnerability results, check for the CVE number on each vulnerability and search the noted CVE number in the [Redhat database](#).

The screenshot shows the Red Hat CVE Database interface. At the top, there's a navigation bar with 'Security Updates' and 'Red Hat CVE Database'. Below this are three main sections: 'Security Advisories', 'Red Hat CVE Database' (highlighted), and 'Security Labs'. A search bar contains 'CVE-2009-3560' and a 'GO' button. To the right of the search bar are filters for severity: 'All' (selected), 'Low', 'Moderate', 'Important', and 'Critical'. Further right is a 'Filter By Year' dropdown set to 'All'. Below the search bar is a table with the following data:

	CVE	Synopsis	Impact	Publish Date
	<a href="#">CVE-2009-3560</a>	The big2_toUtf8 function in lib/xmltok.c in libexpat in Expat 2.0.1, as used in the XML-Twig module for Perl, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with malformed UTF-8 sequences that trigger a buffer over-read, related to the doProlog function in lib/xmlparse.c, a different vulnerability than CVE-2009-2625 and CVE-2009-3720.	Moderate	01 Dec 2009

4. Click the CVE number in the search results to get detailed information.
5. Check the **Affected Packages State** in the Redhat CVE report for **Red Hat Enterprise Linux 6** platform (note that [CentOS 6 is the same as RHEL 6](#)).
6. In the above example CVE-2009-3560, **Red Hat Enterprise Linux 6** platform is **Not affected**. See the following table of affected package states.

### Affected Package States

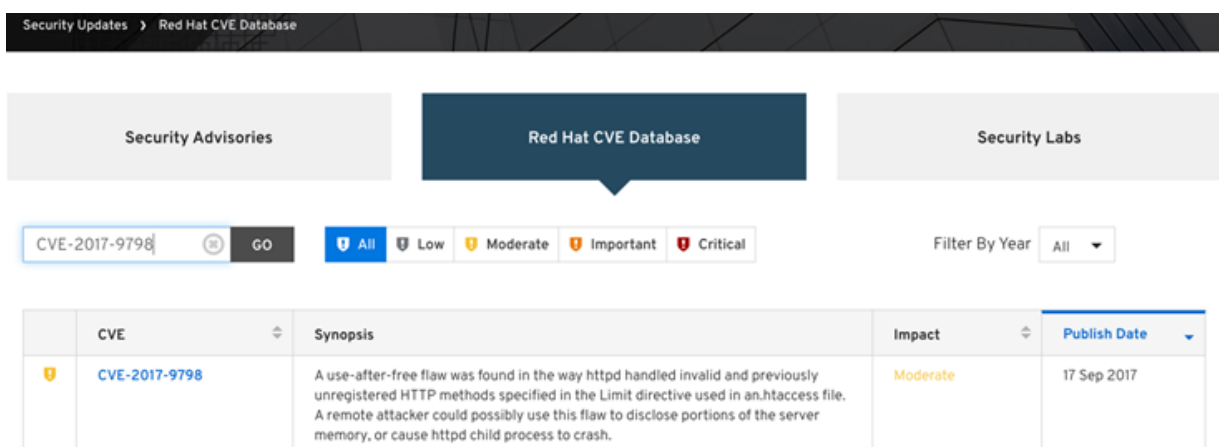
Platform	Package	State
Red Hat Enterprise Linux 7	expat	Not affected
Red Hat Enterprise Linux 6	expat	Not affected
Red Hat Enterprise Linux 6	compat-epa1	Not affected
Red Hat Enterprise Linux 5	xmlrpc-c	Will not fix



7. The Redhat database can return the following types of results:
  - **Not affected** – Vulnerability scanner reported a false alarm.
  - **Will not fix** – Redhat will not fix these vulnerabilities either due to a low CVSS score, or the platform might have reached end of support.
  - **Fixed/Patch available** – Redhat has already provided a fix for these vulnerabilities.
8. You can ignore vulnerabilities that are reported as **Not affected**. You will need to create a vulnerability exception for CVEs that are marked as **Will not fix** by Redhat. For **Fixed** vulnerabilities, follow the instructions in [Validate Redhat Fixed vulnerabilities in FortiSIEM](#).

## Validate Redhat Fixed Vulnerabilities in FortiSIEM

1. From the Vulnerability scanner report, find a CVE number on vulnerability and search for the number in the [Redhat database](#).
2. Perform the following steps if Redhat provides a patch (Security Errata):
  - a. SSH to the FortiSIEM instances and check installed packages.  
**Example:** search for **CVE-2017-9798** in the Redhat database.



- b. Click **CVE-2017-9798** and check the Redhat security errata for **Red Hat Enterprise Linux 6**. See the following table.

### Red Hat Security Errata

Platform	Errata	Release Date
Red Hat JBoss Enterprise Application Platform 6.4	RHSA-2017:3239	2017-11-16
Red Hat Software Collections for Red Hat Enterprise Linux 6 (httpd24-httpd)	RHSA-2017:3018	2017-10-24
Red Hat Enterprise Linux Extended Update Support 6.7 (httpd)	RHSA-2017:3195	2017-11-13
Red Hat Enterprise Linux Extended Update Support 7.2 (httpd)	RHSA-2017:3193	2017-11-13
Red Hat JBoss Web Server	RHSA-2017:3114	2017-11-02
Red Hat JBoss Enterprise Web Server 2 for RHEL 7 Server	RHSA-2017:3113	2017-11-02

Platform	Errata	Release Date
Red Hat JBoss Enterprise Web Server 2 for RHEL 6 Server (httpd)	RHSA-2017:3113	2017-11-02
Red Hat Enterprise Linux 6 (httpd)	RHSA-2017:2972	2017-10-19

- c. Click the [RHSA-2017:2972](#) link, open the **Updated Packages** tab, and note the packages that are updated.

### RHSA-2017:2972 - Security Advisory

Issued: 2017-10-19 Updated: 2017-10-19

Overview

Updated Packages

**Note:** More recent versions of these packages may be available. Click a package name for more details.

#### Red Hat Enterprise Linux Server 6

##### SRPM

httpd-2.2.15-60.el6\_9.6.src.rpm SHA-256: 328aeb280eebb9d347ce5431f9e8d8a36b3c1e0054738ee8738518e5ab45438

##### x86\_64

httpd-2.2.15-60.el6\_9.6.x86\_64.rpm SHA-256: 04c4625a8a3ac4e4dff6b6acb0287dc7339db8cb703d5e860c981a301a67f17fb

httpd-debuginfo-2.2.15-60.el6\_9.6.i686.rpm SHA-256: 7c93c4de01bc9e4e5141bdc670f1e98ed23c941a3b6ccbed421cbe3e3a69ef9b

httpd-debuginfo-2.2.15-60.el6\_9.6.x86\_64.rpm SHA-256: 84e32f93b8c2c8703dfdcabfcd50f599795e97bef8a6ecea677005f93b7285c9

httpd-devel-2.2.15-60.el6\_9.6.i686.rpm SHA-256: 21c9886a4038da0e61e438bee715b4fd7691aea65267bdeb596d2238213d1af6

- d. SSH to the FortiSIEM instance and find installed **httpd** packages (based on the example) by running the `rpm -qa | grep -i httpd` command:

```
[root@sp176 ~]# rpm -qa | grep -i httpd
httpd-2.2.15-69.el6.centos.x86_64
httpd-tools-2.2.15-69.el6.centos.x86_64
```

- e. Check the installed **httpd** package change log to find the **CVE-2017-9798** fixes by running the `rpm -q --changelog httpd | less` command:

```
* Tue Jun 19 2018 Johnny Hughes <johnny@centos.org> - 2.2.15-69
- Roll in centOS Branding

* Mon Feb 19 2018 Luboš Uhliarík <luhliari@redhat.com> - 2.2.15-69
- Resolves: #1471383 - httpd.worker abort()s with misc/apr_reslist.c:159:
  reslist_cleanup: Assertion `rl->ntotal == 0' failed

* Wed Jan 17 2018 Luboš Uhliarík <luhliari@redhat.com> - 2.2.15-68
- Resolves: #1450298 - when ProxyErrorOverride is On, modcluster
  return 503 status code on subsequent requests (2)

* Tue Sep 19 2017 Luboš Uhliarík <luhliari@redhat.com> - 2.2.15-67
- Resolves: #1493060 - CVE-2017-9798 httpd: various flaws

* Wed Jul 26 2017 Luboš Uhliarík <luhliari@redhat.com> - 2.2.15-66
- Resolves: #1463194 - CVE-2017-3167 httpd: ap_get_basic_auth_pw()
  authentication bypass
- Resolves: #1463197 - CVE-2017-3169 httpd: mod_ssl NULL pointer dereference
- Resolves: #1463207 - CVE-2017-7679 httpd: mod_mime buffer overread
- Resolves: #1470748 - CVE-2017-9788 httpd: Uninitialized memory reflection
  in mod_auth_digest

* Fri Jul 07 2017 Luboš Uhliarík <luhliari@redhat.com> - 2.2.15-65
- Related: #1412974 - CVE-2016-8743 httpd: Apache HTTP Request Parsing
  Whitespace Defects

* Thu Jun 29 2017 Luboš Uhliarík <luhliari@redhat.com> - 2.2.15-64
- Resolves: #1463205 - CVE-2017-7668 httpd: ap_find_token() buffer overread
```

- f. In the above example, the **CVE-2017-9798** patch is already available in FortiSIEM.

## Mitigating Found Vulnerabilities

If the CVE number does not exist in the changelog, then follow these steps to perform a FortiSIEM OS update:

1. If the CVE number is not included in the changelog list or the installed package is an older version, perform a FortiSIEM OS update. See [FortiSIEM - OS Update Lifecycle](#).
2. After the FortiSIEM OS update, repeat [Step #2](#) in the previous section, [Validate Redhat Fixed Vulnerabilities in FortiSIEM](#).
3. Contact [FortiSIEM support](#) if the CVE number is not listed in the changelog after the OS update.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.