



Red Hat Insights 2022

Generating Vulnerability Service Reports

Communicate the Exposure of RHEL Systems to CVE Security Vulnerabilities

Red Hat Insights 2022 Generating Vulnerability Service Reports

Communicate the Exposure of RHEL Systems to CVE Security Vulnerabilities

Legal Notice

Copyright © 2022 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Generate vulnerability service reports to communicate the exposure of RHEL systems to CVE security vulnerabilities.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	3
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION	4
CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL VULNERABILITY SERVICE REPORTING	5
CHAPTER 2. EXECUTIVE REPORTS	6
2.1. DOWNLOADING AN EXECUTIVE REPORT	6
2.2. DOWNLOADING AN EXECUTIVE REPORT USING THE VULNERABILITY SERVICE API	6
CHAPTER 3. REPORTS BY CVES	8
3.1. CREATING A PDF REPORT OF CVES	9
CHAPTER 4. EXPORTING VULNERABILITY DATA AS JSON, CSV, OR PDF FILE	11
4.1. EXPORTING CVE DATA FROM THE VULNERABILITY SERVICE	11
CHAPTER 5. REFERENCE MATERIALS	12

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see [our CTO Chris Wright's message](#).

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. To provide feedback, highlight text in a document and add comments.

Prerequisites

- You are logged in to the Red Hat Customer Portal.
- In the Red Hat Customer Portal, the document is in the **Multi-page HTML** viewing format.

Procedure

To provide your feedback, perform the following steps:

1. Click the **Feedback** button in the top-right corner of the document to see existing feedback.



NOTE

The feedback feature is enabled only in the **Multi-page HTML** format.

2. Highlight the section of the document where you want to provide feedback.
3. Click the **Add Feedback** pop-up that appears near the highlighted text.
A text box appears in the feedback section on the right side of the page.
4. Enter your feedback in the text box and click **Submit**.
A documentation issue is created.
5. To view the issue, click the issue link in the feedback view.

CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL VULNERABILITY SERVICE REPORTING

The ability to convey the security exposure of your infrastructure to different stakeholders—DevOps team, security team, executive team—is vital. The vulnerability service enables you to download the following reports to analyze offline or share with others:

- **Executive Reports.** PDF summary and overview of the security vulnerability exposure your infrastructure, intended for executive audiences
- **CVE reports.** PDF report of selected, filtered CVEs to which your infrastructure is exposed, intended to highlight and share vulnerability data
- **Vulnerability data export.** Export of selected CVE data, based on filters you have in place when you perform the export, to a JSON or CSV file

CHAPTER 2. EXECUTIVE REPORTS

You can download a high-level executive report summarizing the security exposure of your infrastructure. Executive reports are two to three-page PDF files, designed for an executive audience, and include the following information:

On page 1

- Number of RHEL systems analyzed
- Number of individual CVEs to which your systems are currently exposed
- Number of security rules in your infrastructure

On page 2

- Percentage of CVEs by severity (CVSS base score) range
- Number of CVEs published by 7, 30, and 90 day time frame
- Top three CVEs in your infrastructure, including security rules and known exploits

On page 3

- Security rule breakdown by severity
- Top 3 security rules, including severity and number of exposed systems

2.1. DOWNLOADING AN EXECUTIVE REPORT

Use the following steps to download an executive report:

Procedure

1. Navigate to the [Red Hat Enterprise Linux > Vulnerability > Reports](#) tab and log in if necessary.
2. On the **Executive report** card, click **Download PDF**.
3. Click **Save File** and click **OK**.

Verification

1. Verify that the PDF file is in your **Downloads** folder or other specified location.

2.2. DOWNLOADING AN EXECUTIVE REPORT USING THE VULNERABILITY SERVICE API

You can download an executive report using the [vulnerability service API](#).

- Request URL: <https://console.redhat.com/api/vulnerability/v1/report/executive>
- Curl:

```
curl -X GET "https://console.redhat.com/api/vulnerability/v1/report/executive" -H "accept: application/vnd.api+json"
```

CHAPTER 3. REPORTS BY CVEs

You can create PDF reports showing a filtered list of CVEs your systems are exposed to. Give each report a relevant name, apply filters, and add user notes to present focused data to specific stakeholders.

You can apply the following filters when setting up the PDF report:

- **Security rules.** Show only CVEs with the security rules label.
- **Known exploit.** Show only CVEs with the Known exploit label.
- **Severity.** Select one or more values: Critical, Important, Moderate, Low, or Unknown.
- **CVSS base score.** Select one or more ranges: All, 0.0-3.9, 4.0-7.9, 8.0-10.0, N/A (not applicable)
- **Business risk.** Select one or more values: High, Medium, Low, Not defined.
- **Status.** Select one or more values: Not reviewed, In review, On-hold, Scheduled for patch, Resolved, No action - risk accepted, Resolved via mitigation.
- **Publish date.** Select from All, Last 7 days, Last 30 days, Last 90 days, Last year, or More than 1 year ago.
- **Applies to OS.** Select the RHEL minor version(s) of systems to filter and view.
- **Tags.** Select groups of tagged systems. For more information about tags and system groups, see [Chapter 4, System tags and groups, *Assessing and Monitoring Security Vulnerabilities on RHEL Systems*](#)

The CVE report lists the CVEs, linking each to the respective CVE page in the Red Hat CVE database so you can learn more about it. The list is ordered primarily by the publish date of the CVE, with the most recently published CVEs at the top of the list.

Example of an Insights Vulnerability CVE report



Prepared 04 Apr 2022 14:35 UTC

Insights Vulnerability CVE Report

This is a summary of CVEs identified by Red Hat that may impact your Red Hat Enterprise Linux (RHEL) systems.

This report includes CVEs with a CVSS base score of 0.0 - 10.0; published anytime.

These CVEs apply to systems in your inventory tagged with `satellite:activation_key=RHEL8_AK`.

The vulnerability service identified 625 CVEs within this criteria that impact at least one of your 17 analyzed RHEL systems. Of the identified CVEs, 4 CVEs have a known exploit.

CVE ID	Publish date	CVSS base score	Severity	Systems exposed	Business risk	Status
CVE-2019-18218	25 Aug 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25038	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25032	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25036	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25042	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25039	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25034	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25035	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2020-9850 Known exploit	09 July 2020	9.8	Moderate	3	Not defined	Not reviewed
CVE-2020-9895	28 July 2020	9.8	Moderate	3	Not defined	Not reviewed

Known exploit: This CVE is identified with a "Known exploit" label because Red Hat has determined this CVE has a public exploit. This CVE is unpatched on your system. CVEs with this label should be addressed with high priority due to the risks posed by them. "Known exploit" does not mean we have taken steps to determine if the CVE has been exploited in your environment.

Security rule: Indicates a security rule associated with this CVE. Security rules are written by Red Hat to help you configure your systems.

3.1. CREATING A PDF REPORT OF CVES

Use the following procedure to create a point-in-time snapshot of CVEs potentially affecting your systems.

Prerequisites

- You must be logged in to [Red Hat Hybrid Cloud Console](#).

Procedure

- Navigate to the [Red Hat Enterprise Linux > Vulnerability > Reports](#) page in the Insights for RHEL application.
- On the **Report by CVEs** card, click **Create report**.
- Make selections as needed in the pop-up card:

Report by CVEs ✕

Report title

Filter CVEs by

Applying to systems in your inventory meeting these criteria

CVE data to include

Sort CVEs by

User notes (optional)

- a. Optionally, customize the report title.
 - b. Under **Filter CVEs by**, click each filter dropdown and select a value.
 - c. Select **Tags** to only include systems in a tagged group of systems.
 - d. Under CVE data to include, **Choose columns** is activated by default, allowing you to deselect columns you do not want to include. Leave all boxes checked, or click **All columns** to show everything.
 - e. Optionally add notes to give the report context for the intended audience.
4. Click **Export report** and allow the application a minute to generate the report.
 5. Select to open or save the PDF file, if your OS asks, and click **OK**.

CHAPTER 4. EXPORTING VULNERABILITY DATA AS JSON, CSV, OR PDF FILE


The vulnerability service enables you to export data for CVEs on systems in your RHEL infrastructure. After applying filters in the vulnerability service to view a specific set of CVEs or systems, you can export data based on those criteria.

These reports are accessible through the Insights for Red Hat Enterprise Linux application and can be exported and downloaded as .csv, .json, or PDF files.

4.1. EXPORTING CVE DATA FROM THE VULNERABILITY SERVICE

Perform the following steps to export select data from the vulnerability service.

Procedure

1. Navigate to the [Red Hat Enterprise Linux > Vulnerability > CVEs](#) page and log in if necessary.
2. Apply filters and use the sorting functionality at the top of each column to locate specific CVEs.
3. Above the list of CVEs and to the right of the Filters menu, click the **Export** icon, , and select **Export to JSON**, **Export to CSV**, or **Export as PDF** based on your download preferences.
4. Select a download location and click **Save**.

CHAPTER 5. REFERENCE MATERIALS

To learn more about the vulnerability service, or other Insights for Red Hat Enterprise Linux services and capabilities, the following resources might also be of interest:

- [Assessing and Monitoring Security Vulnerabilities on RHEL Systems](#)
- [Remediating Security Exposures using the Vulnerability Service and Ansible Playbooks](#)
- [Insights for Red Hat Enterprise Linux Documentation](#)
- [Insights for Red Hat Enterprise Linux Product Support page](#)