Red Hat Insights 2022

Generating Vulnerability Service Reports

Communicate the Exposure of RHEL Systems to CVE Security Vulnerabilities
Communicate the Exposure of RHEL Systems to CVE Security Vulnerabilities
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 HYBRID CLOUD CONSOLE 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 ...................... 10
  4.1. EXPORTING CVE DATA FROM THE VULNERABILITY SERVICE .................... 10

CHAPTER 5. REFERENCE MATERIALS ....................................................... 11
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 HYBRID CLOUD CONSOLE DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so, create a Bugzilla ticket:

1. Go to the Bugzilla website.
2. As the Component, use Documentation.
3. Fill in the Description field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
4. Click Submit Bug.
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:
CHAPTER 3. REPORTS BY CVES

Create PDF reports showing a filtered list of CVEs to which your systems are exposed. 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.

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 showing only RHEL 7.9 systems with security rules

**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; has security rule; and which apply to RHEL 7.9.

The vulnerability service identified 24 CVEs within this criteria that impact at least one of your 342 analyzed RHEL systems.

Of the identified CVEs, 3 CVEs have a known exploit:

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>Publish date</th>
<th>CVSS base score</th>
<th>Severity</th>
<th>Systems exposed</th>
<th>Business risk</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2018-1002105</td>
<td>03 Dec 2018</td>
<td>9.8</td>
<td>Critical</td>
<td>1</td>
<td>Not defined</td>
<td>Not reviewed</td>
</tr>
<tr>
<td>Security rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2020-10713</td>
<td>29 July 2020</td>
<td>8.2</td>
<td>Moderate</td>
<td>1</td>
<td>Not defined</td>
<td>Not reviewed</td>
</tr>
<tr>
<td>Security rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2021-3156</td>
<td>26 Jan 2021</td>
<td>7.8</td>
<td>Important</td>
<td>14</td>
<td>Not defined</td>
<td>Not reviewed</td>
</tr>
<tr>
<td>Known exploit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2021-27965</td>
<td>04 Mar 2021</td>
<td>7.8</td>
<td>Important</td>
<td>9</td>
<td>Not defined</td>
<td>Not reviewed</td>
</tr>
<tr>
<td>Security rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2021-33909</td>
<td>20 July 2021</td>
<td>7.8</td>
<td>Important</td>
<td>49</td>
<td>Not defined</td>
<td>Not reviewed</td>
</tr>
<tr>
<td>Security rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

1. Navigate to the Red Hat Enterprise Linux > Vulnerability > Reports page in the Insights for RHEL application.

2. On the Report by CVEs card, click Create report

3. Make selections as needed in the pop-up card:

   a. Optionally, customize the report title.

   b. Under Filter CVEs by, click each filter dropdown and select a value.

   c. 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.

   d. 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*