Red Hat Insights 1-latest

Generating Vulnerability Service Reports

Communicate the Exposure of RHEL Systems to CVE Security Vulnerabilities

Last Updated: 2024-05-15

Red Hat Insights 1-latest Generating Vulnerability Service Reports

Communicate the Exposure of RHEL Systems to CVE Security Vulnerabilities

Legal Notice

Abstract

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

Table of Contents

CHAPTER 1. OVERVIEW OF INSIGHTS FOR RED HAT ENTERPRISE LINUX VULNERABILITY SERVICE REPORTING 3

CHAPTER 2. EXECUTIVE REPORTS 4

2.1. DOWNLOADING AN EXECUTIVE REPORT 4

2.2. DOWNLOADING AN EXECUTIVE REPORT USING THE VULNERABILITY SERVICE API 4

CHAPTER 3. REPORTS BY CVES 6

CHAPTER 1. OVERVIEW OF INSIGHTS FOR RED HAT ENTERPRISE LINUX 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
- List of CVEs that have advisories

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 Security > 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 System tags and groups