Red Hat Insights 2020-04

Generating Vulnerability Service Reports

Communicate the Exposure of RHEL Systems to CVE Security Vulnerabilities

Last Updated: 2020-05-28
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. Providing Feedback: If you have a suggestion to improve this documentation, or find an error, submit a Bugzilla report at http://bugzilla.redhat.com. Select the Cloud Software Services (cloud.redhat.com) product and use the Documentation component.
# Table of Contents

1. **Vulnerability Service Reporting Overview** ............................................. 3

2. **Executive Reports** .................................................................................. 4
   2.1. Downloading Vulnerability Service Executive Reports .......................... 4
   2.2. Downloading an Executive Report Using the Vulnerability API .......... 4

3. **Exporting Select Vulnerability Data as JSON or CSV File** ...................... 6
   3.1. Exporting a Vulnerability Service Report ........................................... 6

4. **Reference Materials** ................................................................................ 7

5. **Important Changes with the 2020-04 Release of Red Hat Insights** ........... 8
CHAPTER 1. VULNERABILITY SERVICE REPORTING OVERVIEW

Reporting infrastructure security status is a key aspect of vulnerability management. The ability to convey the security exposure of your infrastructure to different stakeholders needing different levels of information is vital. From your DevOps team, to the security team, to your executive team, you need to be able to provide your stakeholders the information they need.

The Vulnerability service enables you to download reporting for your systems to analyze offline or share with others. The following reporting options are currently supported:

- **Executive Reports.** PDF summary and overview of your infrastructure security exposure intended for executive audiences
- **Vulnerability data export.** JSON or CSV export of select CVE data, based on filters you have in place when you perform the export

**NOTE**

New reporting capabilities are coming soon.
CHAPTER 2. EXECUTIVE REPORTS

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

- Number of RHEL systems with one or more CVEs
- Number of CVEs to which your systems are currently exposed
- Percentage of CVEs, by severity (CVSS base score range)
- Number of CVEs published in the past 7, 30, or 90-day time frame
- Top three CVEs in your infrastructure based on highest CVSS base score range (8-10) with the greatest number of systems exposed

2.1. DOWNLOADING VULNERABILITY SERVICE EXECUTIVE REPORTS

Use the following steps to download an executive report:

Procedure

1. Navigate to the Vulnerability service > CVEs tab and log in if necessary.
2. Click the Download executive report link located in the upper-right corner of the page.
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 API

You can download an executive report using the Vulnerability API.

- Request URL: https://cloud.redhat.com/api/vulnerability/v1/v1/report/executive
- Curl:
CHAPTER 3. EXPORTING SELECT VULNERABILITY DATA AS JSON OR CSV FILE

The Vulnerability service enables you to export and download reports showing CVEs impacting systems in your RHEL infrastructure. Prefilter CVEs by criticality or CVSS base score, for example, and export a CSV or JSON file with data for those CVEs and impacted systems. Then share that data with other stakeholders in your organization.

3.1. EXPORTING A VULNERABILITY SERVICE REPORT

Perform the following steps to export select data from the Vulnerability service:

Procedure

1. Navigate to the Vulnerability service > CVEs tab and log in if necessary.

2. Apply filters and use the sorting functionality at the top of each column to locate CVEs of interest.

3. Above the list of CVEs and to the right of the Filters menu, click the more-actions icon (three vertical dots) and select Export as JSON or Export as CSV, based on your download preferences.

4. Select a download location and click Save.
CHAPTER 4. REFERENCE MATERIALS

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

Documentation

- *Assessing and Monitoring Vulnerabilities on RHEL Systems*
- *Remediating Security Exposures using Vulnerability and Ansible Playbooks*
- Red Hat Insights Documentation
- Red Hat Insights Product Support page
CHAPTER 5. IMPORTANT CHANGES WITH THE 2020-04 RELEASE OF RED HAT INSIGHTS

The 2020-04 release of Red Hat Insights includes significant changes to the application features and services.

Changes to the Red Hat Insights application

The Red Hat Insights application now includes the services that were previously bundled with the Cloud Management Services for RHEL application, and were part of the Red Hat Smart Management bundle, along with Red Hat Satellite.

The former cloud management services, plus a couple of new services, are now included in the value that Insights brings to each Red Hat Enterprise Linux (RHEL) subscription.

Insights Advisor

The tools and capabilities that constituted Red Hat Insights prior to this release are now available as the Advisor service. The rules that have always been the currency of Insights are now called Advisor Recommendations.

Insights security rules have moved

The CVE security rules that were previously curated by the Insights rules team are now included with all other Red Hat CVEs in the Vulnerability service. Security rules are high profile CVEs, some of which have been through the Customer Security Awareness Program. They are identifiable in the Vulnerability service by a security rule icon. You can also filter security rules in the Vulnerability service.

Services included with Red Hat Insights

The services included with Red Hat Insights in the 2020-04 release are:

- **Advisor.** Identify and fix configuration issues that can negatively impact the availability, performance, stability, and security of RHEL systems.

- **Vulnerability.** Assess and monitor the exposure of your RHEL environment to CVEs and security rules.

- **Compliance.** Assess and monitor the compliance of your RHEL systems with SCAP security policies.

- **Patch.** Enable consistent patch workflows for RHEL systems across the open hybrid cloud.

- **Drift.** Compare system configurations of a system over time, or to other systems and baselines, to identify discrepancies in your environment and perform drift analysis.

- **Policies.** Evaluate and react to system configuration changes in your environment.

The integrated tools that work with each of the services above are:

- **Inventory.** Topological inventory of RHEL systems under Red Hat Insights management

- **Remediations.** Repository of Ansible Playbooks that you create and manage using Red Hat Insights

- **Subscription Watch.** Comprehensive, product-by-product, account-level subscription reporting service across hybrid cloud deployments
Resources

- Red Hat Insights Product Support page
- Red Hat Insights Documentation
- Red Hat Insights Release Notes
- Red Hat Insights blog channel