Red Hat Insights 2020-10

Generating Vulnerability Service Reports

Communicate the Exposure of RHEL Systems to CVE Security Vulnerabilities

Last Updated: 2020-11-02

Red Hat Insights 2020-10 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. 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

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
- **CVE reports.** PDF report of select CVEs potentially impacting your infrastructure
- **Vulnerability data export.** JSON, CSV, or PDF export of select CVE data, based on filters you have in place when you perform the export, and which can be used in spreadsheets, for example.

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:

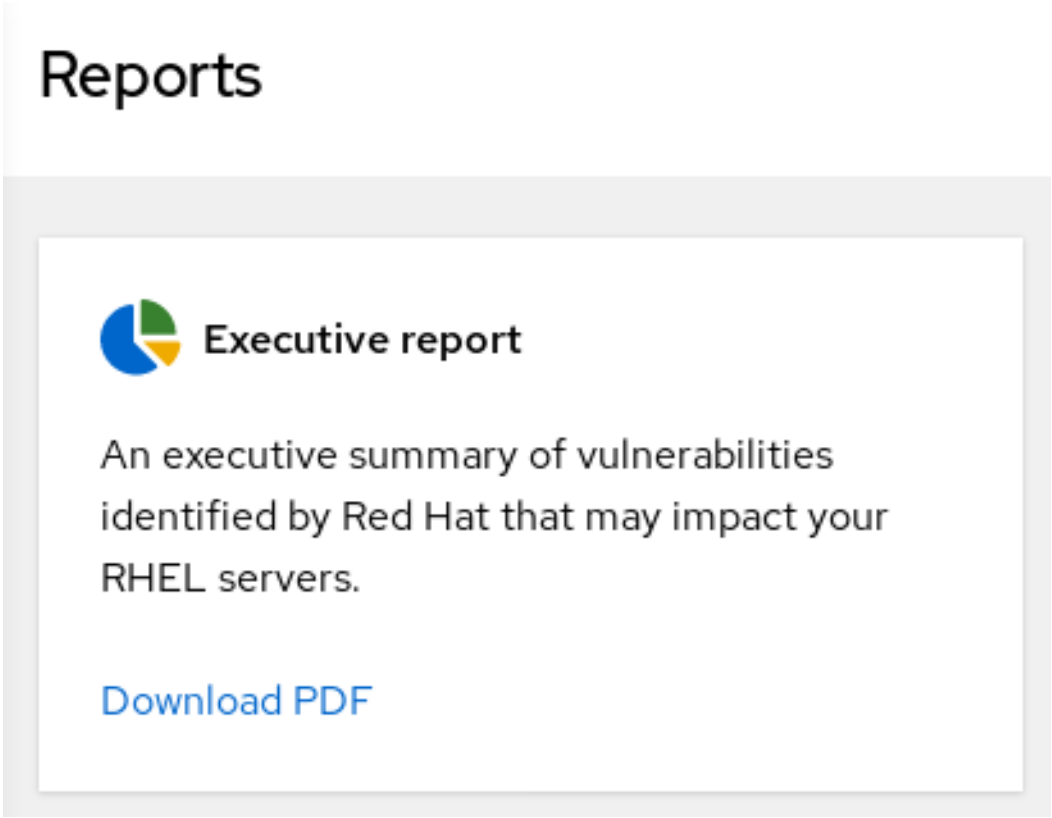
- Number of RHEL systems with one or more CVEs
- Number of CVEs to which your systems are currently exposed
- Percentage of CVEs, by severity (CVSS base score range)
- Number of CVEs published in the past 7, 30, or 90-day time frame
- Top three CVEs in your infrastructure based on highest CVSS base score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

2.1. DOWNLOADING AN EXECUTIVE REPORT

Use the following steps to download an executive report:

Procedure

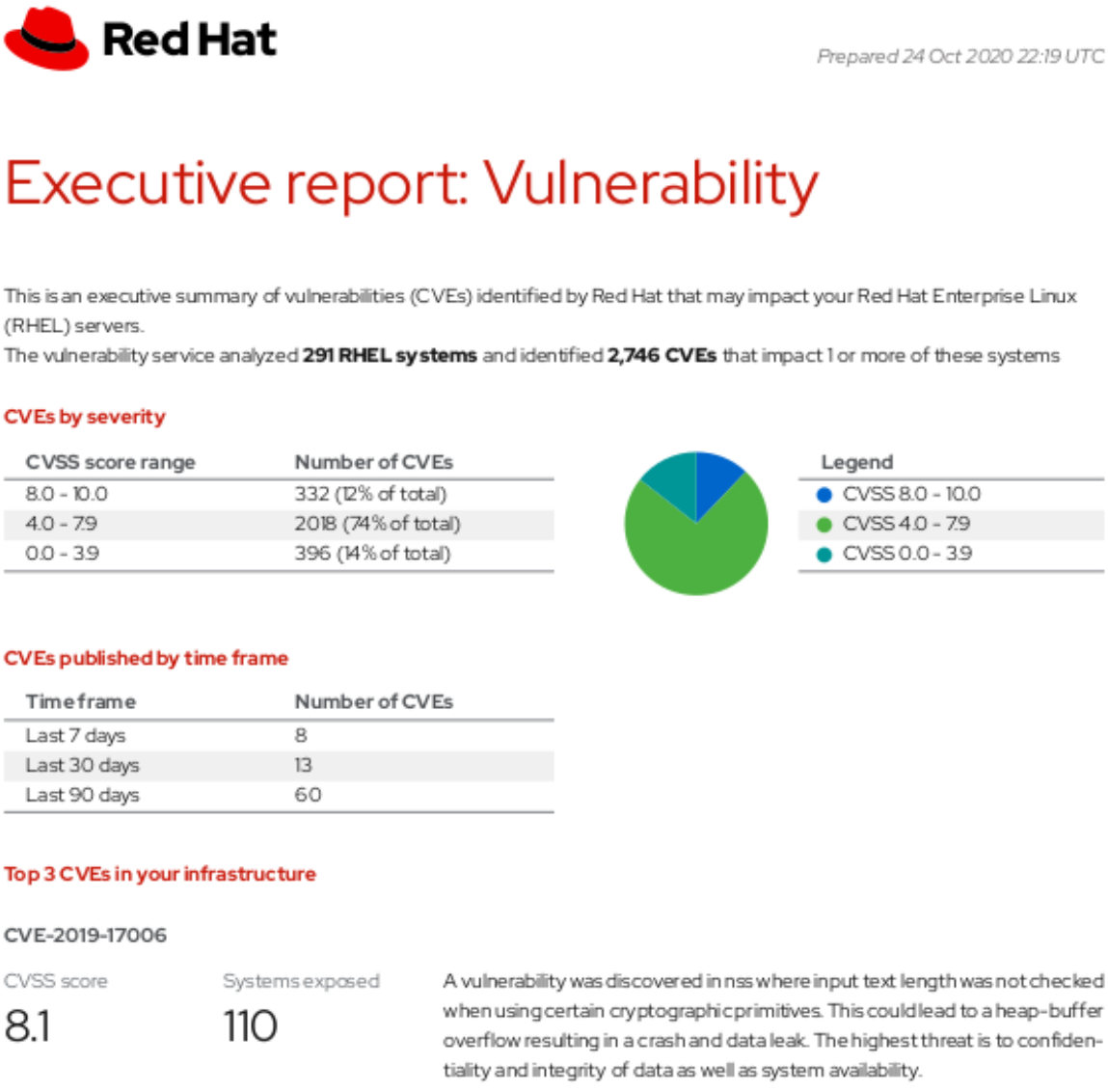
1. Navigate to the Vulnerability service > Reports tab and log in if necessary.
2. On the Reports page, click the **Download PDF** link on the **Executive report** card.



3. Click **Save File** and click **OK**.

Verification

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



Red Hat

Prepared 24 Oct 2020 22:19 UTC

Executive report: Vulnerability

This is an executive summary of vulnerabilities (CVEs) identified by Red Hat that may impact your Red Hat Enterprise Linux (RHEL) servers.
The vulnerability service analyzed **291 RHEL systems** and identified **2,746 CVEs** that impact 1 or more of these systems

CVEs by severity

CVSS score range	Number of CVEs
8.0 - 10.0	332 (12% of total)
4.0 - 7.9	2018 (74% of total)
0.0 - 3.9	396 (14% of total)

CVEs published by time frame

Time frame	Number of CVEs
Last 7 days	8
Last 30 days	13
Last 90 days	60

Top 3 CVEs in your infrastructure

CVE-2019-17006

CVSS score 8.1

Systems exposed 110

A vulnerability was discovered in nss where input text length was not checked when using certain cryptographic primitives. This could lead to a heap-buffer overflow resulting in a crash and data leak. The highest threat is to confidentiality and integrity of data as well as system availability.

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:

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

CHAPTER 3. REPORTS BY CVES

You can create point-in-time PDF reports showing CVEs potentially impacting your systems. Select types of CVEs, filtered by severity or CVSS base score, for example, and present curated, focused data to specific stakeholders. Prior to creating the report, you can make the following customizations to the list of CVEs:

- Change the default title, Insights Vulnerability CVE Report, to a title you choose.
- Choose whether to include only CVEs with associated security rules.

NOTE

For more information about security rules, see the Security Rules section in Assessing and Monitoring Security Vulnerabilities on RHEL Systems .

- Choose which columns to include. The following report columns are selected by default; however, you can clear any as needed, except CVE ID:
  - CVE ID (required)
  - Publish Date
  - Severity
  - CVSS base score
  - Count of exposed systems
  - Business risk
  - Status
- You can apply the following filters to the columns:
  - Publish Date. Select a range of time.
  - Severity. Select one or more severity ratings.
  - CVSS base score. Specify a minimum score to maximum score range.
  - Business risk. Select one or more business risk ratings.
  - Status. Select the status of review and resolution.

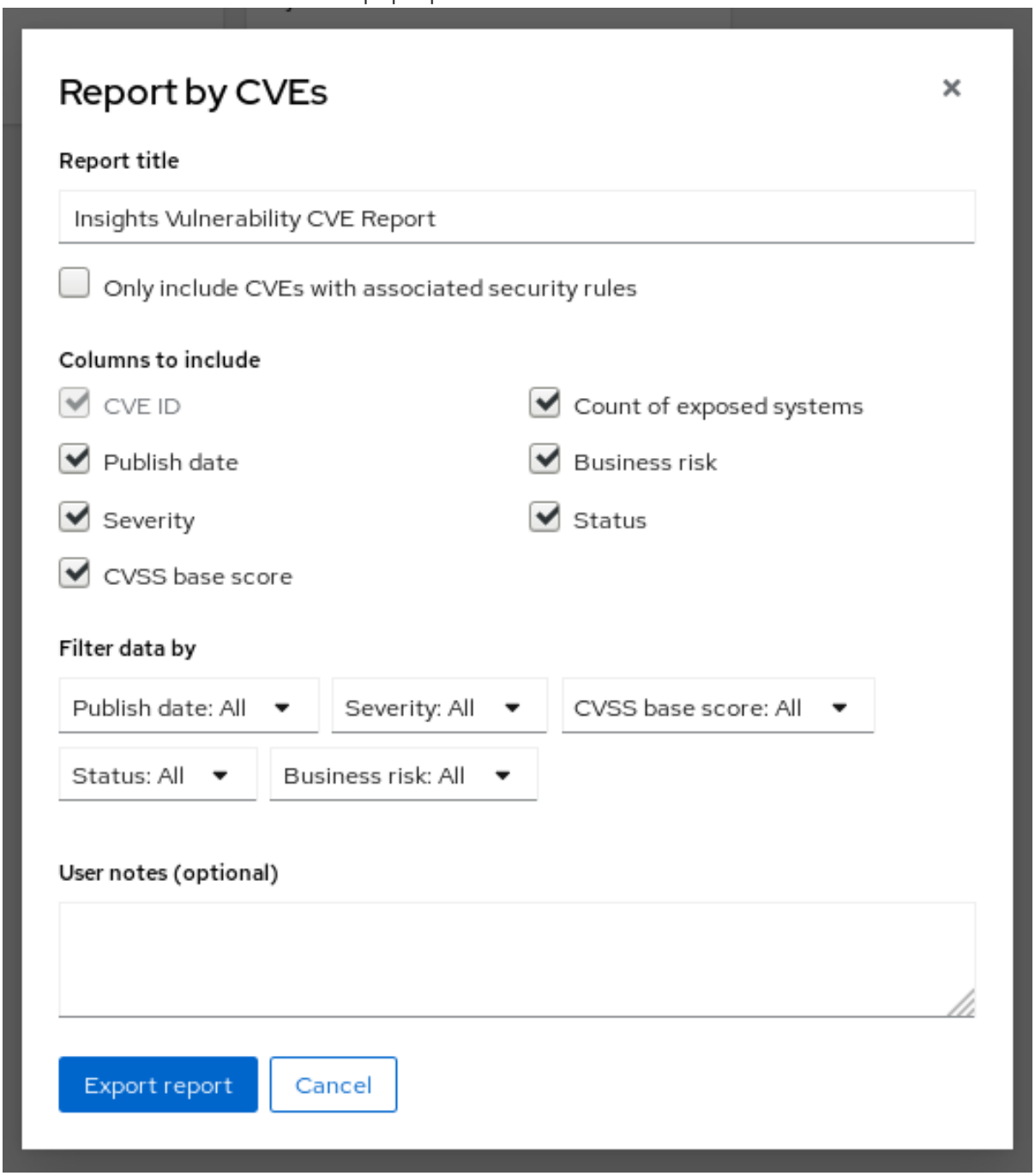
The resulting PDF lists the CVEs and link to the respective CVE page in the Red Hat CVE database so you can learn more about each one. The list is ordered primarily by the publish date of the CVE, with the most recently published CVEs at the top of the list.

3.1. EXPORTING A CVE REPORT TO PDF

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

Procedure

1. Navigate to Vulnerability service > Reports in the Insights application. Log in if necessary.
2. On the **Report by CVEs** card, click **Create report**.
3. Make selections as needed in the pop-up card:



   a. Customize the report title.
   b. Choose whether to **Only include CVEs with associated security rules**

NOTE

For more information about security rules, see the Security Rules section in Assessing and Monitoring Security Vulnerabilities on RHEL Systems .

   c. Select from the **Columns to include** options.
   d. From the **Filter data by** dropdown lists, select ranges for the available parameters.

e. Add optional **User notes** to provide needed context for stakeholders.

4. Click **Export report** and allow the application a minute to generate the report.
5. Select to **Open** or **Save file** and click **OK**.

Verification

1. Navigate to the saved PDF location and view the CVEs report.

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

The Vulnerability service enables you to export data for active CVE hits on systems in your RHEL infrastructure. After applying filters in the Vulnerability UI to view a specific set of CVEs or systems, you can export data for those criteria, allowing you to filter which CVE data is shown. You can prefilter CVEs by criticality or CVSS base score, for example, and generate a report that shows only those relevant CVEs.

These reports are accessible through the UI and can be exported and downloaded as .csv, .json, or PDF files.

4.1. 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 page 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 **Export** icon,  , and select **Export as JSON**, **Export as 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 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