Red Hat Insights 2020-04

Assessing and Monitoring Security Vulnerabilities on RHEL Systems

Understanding your Environmental Exposure to Potential Security Threats
Understanding your Environmental Exposure to Potential Security Threats
Abstract

Use the Vulnerability service to assess and monitor the status of security vulnerabilities on your RHEL systems, understand the level of exposure of your infrastructure, and plan a course of action. 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

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAPTER 1. VULNERABILITY SERVICE OVERVIEW</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>1.1. VULNERABILITY SERVICE REQUIREMENTS AND PREREQUISITES</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 2. COMMON VULNERABILITIES AND EXPOSURES (CVES)</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2.1. SECURITY RULES</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 3. VIEWING AND TRIAGING THE SECURITY VULNERABILITIES IMPACTING YOUR RHEL SYSTEMS</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>3.1. VIEW A LIST OF CVES IMPACTING SYSTEMS IN YOUR INVENTORY</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>3.2. VIEW A LIST OF SYSTEMS AND THE CVES IMPACTING EACH SYSTEM</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 4. REFINING AND SIMPLIFYING YOUR VULNERABILITY DATA</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>4.1. DEFINING A BUSINESS RISK FOR A CVE</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>4.2. EXCLUDING SYSTEMS FROM VULNERABILITY SERVICE ANALYSIS</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>4.2.1. Showing previously excluded systems</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>4.2.2. Resuming vulnerability analysis for a system</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>4.3. SETTING A STATUS FOR A CVE</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>4.3.1. Setting a status for a CVE on all affected systems</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>4.3.2. Setting a status for a CVE and system pairing</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>4.4. USING THE SEARCH BOX</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>4.5. APPLYING FILTERS</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>4.6. SORTING CVE LIST DATA</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 5. REFERENCE MATERIALS</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>CHAPTER 6. IMPORTANT CHANGES WITH THE 2020-04 RELEASE OF RED HAT INSIGHTS</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 1. VULNERABILITY SERVICE OVERVIEW

The Vulnerability service enables quick assessment and efficient monitoring of the exposure of your RHEL infrastructure to Common Vulnerabilities and Exposures (CVEs) so you can better understand your most critical issues and systems and effectively manage remediations.

With your data uploaded to the Vulnerability service, you can filter and sort groups of systems and CVEs to optimize your views. You can also add context to individual CVEs when they pose an extraordinary risk to systems. After gaining an understanding of your risk exposure, create Ansible Playbooks to remediate issues to secure your organization and report on the status of the CVEs to appropriate stakeholders.

This documentation describes key features of the Vulnerability service and how to use them. For more information about remediations and reporting, see the following documentation:

- Remediating Security Exposures using Vulnerability and Ansible Playbooks
- Generating Vulnerability Reports

1.1. VULNERABILITY SERVICE REQUIREMENTS AND PREREQUISITES

The Vulnerability service is available for all supported versions of RHEL 6, 7, and 8. The following conditions must be met before you can use the Vulnerability service:

- Each system has the Insights client installed and registered to the Insights service. Follow the Get Started instructions to install the client and register your system(s).
- The Vulnerability service is fully supported for RHEL systems managed by Red Hat Subscription Manager (RHSM) and Satellite 6 and later. Using any other means to obtain package updates, other than Satellite 6 with RHSM or RHSM registered with subscription.redhat.com (Customer Portal), can lead to misleading results.
- Vulnerability service remediations are not fully supported and may not work properly on Satellite 5 and Spacewalk-hosted RHEL systems.
CHAPTER 2. COMMON VULNERABILITIES AND EXPOSURES (CVES)

Common Vulnerabilities and Exposures (CVES) are security vulnerabilities identified in publicly released software packages. CVEs are identified and listed by the National Cybersecurity FFRDC (NCF), the federally funded research and development center operated by the Mitre Corporation, with funding from the National Cyber Security Division of the United States Department of Homeland Security. The complete list of CVEs is available at https://cve.mitre.org.

The Vulnerability service identifies CVEs impacting your RHEL systems and gives you the information you need to understand their potential risk and how to resolve them.

IMPORTANT

The Vulnerability service does not contain every CVE included in the list of entries at https://cve.mitre.org. Only Red Hat CVEs, those CVEs for which Red Hat issues security advisories (RHSAs), are included in the Vulnerability service.

2.1. SECURITY RULES

What is a security rule and what is its significance?

Security rules are Red Hat CVEs, previously identified by the Red Hat Insights application (now Advisor service), deemed worthy of additional visibility due to the risk and exposure associated with them.

These are security flaws that usually get significant coverage in the press. These CVEs have been scrutinized by the Red Hat Product Security team, which uses the Customer Security Awareness (CSAw) Program workflow to manually create algorithms to help determine your RHEL environment exposure, enabling you to take the appropriate action to protect your organization.

If the Vulnerability service identifies a system or systems as being exposed to a security rule, there is the potential for elevated security risk on those systems and issues should be addressed with urgency.

NOTE

Not all systems that are exposed to a given CVE will be exposed to a security rule associated with that CVEs. In other words, while a CVE may be applicable to 10 systems, the number of systems exposed to a security rule for that CVE, if one exists, can be a subset of the 10 systems. In such a scenario, the urgency to address systems with the security rule applying to them should be higher priority.

Where can I find Security rules?

The security rules are now part of the Vulnerability service, along with other Red Hat CVEs, providing complete coverage of all CVEs that may impact your RHEL systems. The CVEs that have security rules are identifiable by the security-rule icon located to the left of the CVE ID as well as next to systems that have current security rule vulnerabilities.
NOTE

You can also retrieve a list of the security rules that are applicable to at least one of your systems with the following API call:

https://cloud.redhat.com/api/vulnerability/v1/vulnerabilities/cves?page=1&page_size=100&security_rule=true&show_all=true&sort=-public_date

A Red Hat CVE can have multiple security rules associated with it and the opposite is also true. If a CVE has multiple security rules, it is reflected in the CVE details view.

A CVE with multiple security rules is shown in the following example:
If a security rule has multiple CVEs associated to it, it will be visible as follows:

**CVE-2019-1477**

**Business risk**
- Not defined

**Status**
- Not reviewed

An integer overflow flaw was found in the way the Linux kernel’s networking subsystem processed TCP Selective Acknowledgment (SACK) segments. While processing SACK segments, the Linux kernel’s socket buffer (skb) data structure becomes fragmented. Each fragment is about TCP maximum segment size (MSS) bytes. To efficiently process SACK blocks, the Linux kernel merges multiple fragmented skb’s into one, potentially overflowing the variable holding the number of segments. A remote attacker could use this flaw to crash the Linux kernel by sending a crafted sequence of SACK segments on a TCP connection with small value of TCP MSS, resulting in a denial of service (DoS).

**Published date:** 17 June 2019

View in Red Hat CVE database [here](#).
CHAPTER 3. VIEWING AND TRIAGING THE SECURITY VULNERABILITIES IMPACTING YOUR RHEL SYSTEMS

To view the CVEs that are impacting your RHEL inventory, there are two approaches that you can use:

3.1. VIEW A LIST OF CVES IMPACTING SYSTEMS IN YOUR INVENTORY

Procedure

1. Navigate to the **Vulnerability service > CVEs** tab and log in if necessary.
2. Optionally, apply filters or sort results to refine your view.
3. Click on a CVE to view the description, links to more information, impact severity rating, business risk, status, and Common Vulnerability Scoring System (CVSS) base score.
4. Scroll down to view the list of impacted systems with exposure to that CVE.
5. Click on a system to view information about that system, all impacting CVEs, and to select CVEs to remediate with Ansible.

3.2. VIEW A LIST OF SYSTEMS AND THE CVES IMPACTING EACH SYSTEM

Procedure

1. Navigate to **Vulnerability service > Systems** and log in if necessary.
2. Click on a system to view system information and a list of CVEs to which the system is exposed.
3. Optionally, apply filters or sort results to refine your view of impacting CVEs.
4. Select an individual CVE to see more information about it.
CHAPTER 4. REFINING AND SIMPLIFYING YOUR VULNERABILITY DATA

The Vulnerability service enables many ways to refine the views of your data, helping you focus on your most critical issues. The sections in this chapter describe the organization of your data and the sorting, filtering, and contextual features you can use to refine your results.

4.1. DEFINING A BUSINESS RISK FOR A CVE

The Vulnerability service allows you to define the business risk of a CVE with the following options: High, Medium, Low, or Not Defined (default).

While the list of CVEs shows the severity of each one, assigning a business risk lets you rank CVEs based on the impact they could have on your organization. This can give you more control in managing your risk efficiently in a large environment and enable you to make better operational decisions.

By default, the business risk field for a specific CVE is set to Not Defined. After you set the business risk, it is visible in the Vulnerability service > CVEs list, next to each CVE. Business risk is also visible on the details card for each CVE, which shows more information and lists affected systems.

Procedure for setting a business risk for a single CVE

The following procedure will set the business risk on a single CVE. The business risk for that CVE will be the same on all systems impacted by it.

1. Navigate to the Vulnerability service > CVEs tab and log in if necessary.
2. Identify a CVE for which you want to set a business risk.
3. Perform the following steps for each CVE:
   a. Click the more-actions icon (three vertical dots) on the right end of the CVE row and click Edit business risk.
   b. Set a business risk value to the appropriate level and, optionally, add a justification for your risk assessment.
   c. Click Save.

Procedure for setting a business risk for multiple CVEs

The following procedure will set the same business risk on multiple CVEs that you select.

1. Navigate to Vulnerability service > CVEs and log in if necessary.
2. Check the boxes for the CVEs on which you want to set a business risk.
3. Perform the following steps to set a business risk:
   a. Click the more-actions icon (three vertical dots) to the right of the Filters dropdown menu in the toolbar and click Edit business risk.
b. Set an appropriate business risk value and, optionally, add a justification for your risk assessment.

c. Click Save.

4.2. EXCLUDING SYSTEMS FROM VULNERABILITY SERVICE ANALYSIS

The Vulnerability service allows you to exclude specific systems from vulnerability analysis. This can save you the time and attention required to review and re-review issues on systems that are not relevant to your organization’s goals.

As an example, if you have the following category of servers: QA, Dev, and Production, you may not care to review the vulnerabilities for your QA servers and therefore want to exclude these systems from the analysis performed by the Vulnerability service.

When you exclude systems from vulnerability analysis, the Insights client still runs per schedule on the system, but the results for the system are not visible in the Vulnerability service. The continued operations of the client ensure that other Red Hat Insights services can still upload the data they need. It also means that you can still view results for those systems using filtering.

Complete the following steps to exclude selected RHEL systems from Vulnerability service analysis:

Procedure

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

2. Check the box for each system you want to exclude from vulnerability analysis.

3. Click the more-actions icon in the toolbar, at the top of the list of systems, and select Exclude systems from vulnerability analysis.
4.2.1. Showing previously excluded systems

**Procedure**

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

2. Click the more actions icon in the toolbar, at the top of the list of systems, and select **Show systems excluded from analysis**.

3. See systems excluded from vulnerability analysis. This can be verified by the value of **Excluded** in the **Number of CVEs** column.

4.2.2. Resuming vulnerability analysis for a system

**Procedure**

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

2. Click the more actions icon in the toolbar, at the top of the list of systems, and select **Show systems excluded from analysis**.

3. In the list of results, check the box for each system for which you want to resume vulnerability analysis.

4. Click the more actions icon again and select **Resume analysis for system**.

4.3. SETTING A STATUS FOR A CVE

Another method of managing CVEs impacting your systems is by setting a status for CVEs. The Vulnerability service enables the following ways of setting a status for a CVE:

- Set a status for a CVE for all systems.
- Set a status for a specific CVE + system pair.

Statuses are preset and include the following options:
- Not reviewed (default)
- In-review
- On-hold
- Scheduled for patch
- Resolved
- No action - risk accepted
- Resolved via mitigation

Setting a status for a CVE can lead to better triaging through its lifecycle, from finding it to remediating it. Defining a status allows your organization to keep better tabs on where the most critical CVEs are in their lifecycle and where you should focus your efforts to address the most critical issues per your business need. The status for a CVE is visible in all CVE tables in the Vulnerability service and in individual CVE views.

4.3.1. Setting a status for a CVE on all affected systems

Use the following procedure to set a status for a CVE and have that status apply to that CVE on all of the systems it impacts:

**Procedure**

1. Navigate to the Vulnerability service > CVEs tab and log in if necessary.
2. Click the more-actions icon located on the right end of the CVE row and select **Edit status**.
3. Select the appropriate status and, optionally, enter a rationale for your decision in the **Justification** text box.
4. Check **Do not overwrite individual system status** if there are statuses set for this CVE on individual systems and that you want to preserve. Otherwise, leave the box unchecked to apply this status to all of the systems it is impacting.
5. Click **Save**.

4.3.2. Setting a status for a CVE and system pairing

Use the following procedure to set a status on a CVE and system pairing:

**Procedure**

1. Navigate to the Vulnerability service > Systems tab and log in if necessary.
2. Identify the system and click the system name to open it.
3. Select a CVE from the list and check the box next to the CVE ID.
4. Click the more-options icon in the toolbar and select **Edit status**.
5. In the popup card, take the following actions:
   a. Optionally, check the **Use overall CVE status** box to make this CVE status apply to this
a. Optionally, check the Use overall CVE status box to make this CVE status apply to this CVE and all the systems that it affects.

b. Set a status for the CVE and system pair.

c. Optionally, enter a justification for your status determination.

6. Click **Save**.

### 4.4. USING THE SEARCH BOX

The search function in the Vulnerability service works in the context of the page you are viewing.

- **CVEs tab.** The search box is located at the top of the list in the toolbar. CVE IDs and descriptions can be searched.

- **Systems tab.** The search box is located in the toolbar at the top of the list. System UUIDs can be searched.

### 4.5. APPLYING FILTERS

Filtering is available from the CVEs list and, after clicking an individual CVE ID, from the list of affected systems. Filtering will narrow the visible list of CVEs and help you focus on the issues you’re most interested in. When you select filters, they are visible below the Filters menu. Click on the **X** on a filter to remove it, or click **Clear filters** to remove all current filters.

#### CVE filters

The following filters are accessible from the CVEs tab:

- **Hide CVEs that do not affect my inventory.** This omits CVEs that your systems are scanned for but do not affect.

- **Security rules.** Show only CVEs that have security rules associated with them.

- **Impact.** The impact level will help you gauge your potential risk and triage remediation actions.

- **CVSS base score.** Click one or more radio buttons to include or eliminate CVEs in a base score range.

- **Business risk.** This adds another layer of context to the potential risk of a CVE on an affected system.

- **Status.** Status of review or resolution.

- **Publish date.** Exclude newer or older CVEs based on your criteria.

### 4.6. SORTING CVE LIST DATA
The sorting functions in the Vulnerability service differ based on the context of the information you are viewing.

In the CVEs tab, you can apply sorting to the following columns:

- CVE ID
- Publish date
- Impact
- CVSS base score
- Systems exposed
- Business risk
- Status

After you select a system in the Systems tab, the list of CVEs allows the following sorting options:

- CVE ID
- Publish date
- Impact
- CVSS base score
- Business risk
- Status
CHAPTER 5. REFERENCE MATERIALS

To learn more about the Vulnerability service, see the following resources:

- *Remediating Security Exposures using Vulnerability and Ansible Playbooks*
- *Generating Vulnerability Reports*
- *Red Hat Insights Documentation*
- *Red Hat Insights Product Support page*
CHAPTER 6. 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