Red Hat Insights 2022

Assessing and Monitoring Security Vulnerabilities on RHEL Systems

Understanding your Environmental Exposure to Potential Security Threats

Last Updated: 2022-06-16

Red Hat Insights 2022 Assessing and Monitoring Security Vulnerabilities on RHEL Systems

Understanding your Environmental Exposure to Potential Security Threats

Legal Notice

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.

Table of Contents

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 DOCUMENTATION

We appreciate your feedback on our documentation. To provide feedback, highlight text in a document and add comments.

Prerequisites

- You are logged in to the Red Hat Customer Portal.
- In the Red Hat Customer Portal, the document is in the **Multi-page HTML** viewing format.

Procedure

To provide your feedback, perform the following steps:

1. Click the **Feedback** button in the top-right corner of the document to see existing feedback.

NOTE

The feedback feature is enabled only in the **Multi-page HTML** format.

2. Highlight the section of the document where you want to provide feedback.
3. Click the **Add Feedback** pop-up that appears near the highlighted text.
   A text box appears in the feedback section on the right side of the page.
4. Enter your feedback in the text box and click **Submit**.
   A documentation issue is created.
5. To view the issue, click the issue link in the feedback view.

CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL VULNERABILITY SERVICE

The vulnerability service enables quick assessment and comprehensive 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 refine and 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, report on the status of the CVEs to appropriate stakeholders, then create Ansible Playbooks to remediate issues to secure your organization and.

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

- *Remediating Security Exposures using the Vulnerability Service and Ansible Playbooks*
- *Generating Vulnerability Service Reports*

1.1. INSIGHTS FOR RHEL 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 for RHEL application.** Follow the Insights for Red Hat Enterprise Linux, 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 Management (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.**
- **Some features require special privileges provided by your organization administrator.** Specifically, the ability to view Red Hat Security Advisories (RHSAs) associated with certain CVEs and systems, and to view and patch those vulnerabilities in the Insights for Red Hat Enterprise Linux patch service, requires permissions granted through user access.

1.2. USER ACCESS FOR VULNERABILITY SERVICE USERS

Before you can access certain features in the Insights for Red Hat Enterprise Linux application, you must have the correct permissions, which are granted in Red Hat Hybrid Cloud Console > User Access > Groups. An Organization Administrator or **User Access administrator** must add you as a member to a User Access group with the required roles.

By default, User Access on the Red Hat Hybrid Cloud Console has preconfigured **Vulnerability administrator** (all access) and **Vulnerability viewer** (read-only access) roles. If your organization determines that the default roles provide insufficient access, a **User Access administrator** can configure a custom role to provide the specific permissions required by a set of users.

The following sections in this chapter describe each of the default roles for vulnerability service users.

IMPORTANT

Changes to User Access must be performed by an Organization Administrator on your Red Hat account, or by an account user who is a member of a User Access group with the **User Access administrator** role.

Additional resources

- *User Access Configuration Guide for Role-based Access Control (RBAC)*

1.2.1. Vulnerability administrator role

The **Vulnerability administrator** role is a default role in the **Default access group**. All Insights for Red Hat Enterprise Linux users on your account are members of the **Default access group** by default. In its default configuration, members of a group with the **Vulnerability administrator** role have access to all vulnerability service resources.

Your organization may decide that the default role is too limited, or too permissive. To limit access to some features, or to add additional permissions, a **User Access administrator** can customize the role and configure it with whatever permissions are required. By customizing the preconfigured role, the **Default access group** is replaced.

1.2.2. Vulnerability viewer role

In its default configuration, the **Vulnerability viewer** role can read any vulnerability service resource. This is a preconfigured role but is not included in the **Default access group**. The **Vulnerability viewer** role includes the following permissions:

- View and triage all vulnerability service results, pages, and lists.
- View which systems have been opted out of reporting results to Insights for Red Hat Enterprise Linux.
- Set filters and export data for .JSON and .CSV output.
- View and create advanced reports in Red Hat Enterprise Linux > Vulnerability > Reports .

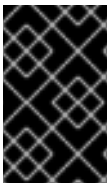
If your organization determines that the default configuration of the Vulnerability viewer role is inadequate, a User Access administrator can create a custom role with the specific permissions required.

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.

By highlighting CVEs with publicly known exploits and security rules associated with CVEs, the vulnerability service surfaces enhanced threat intelligence to aid in determining which CVEs pose the greatest potential risk to RHEL environments, enabling our users to effectively prioritize and address their most critical issues first.



IMPORTANT

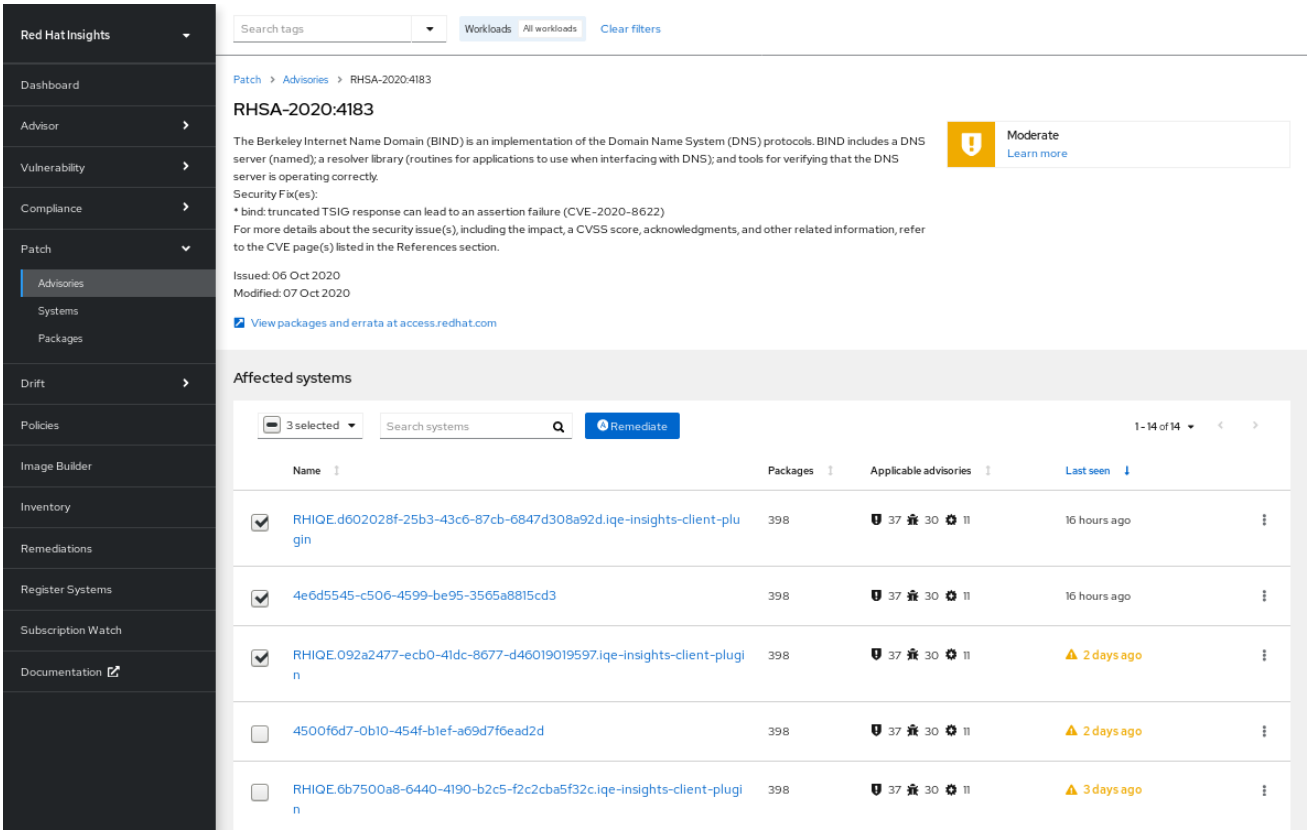
The vulnerability service does not contain every CVE included in the list of entries at https://cve.mitre.org. Only Red Hat CVEs, those CVEs for which Red Hat issues security advisories (RHSAs), are included in the vulnerability service.

2.1. RED HAT SECURITY ADVISORIES (RHSAS)

Red Hat Security Advisory (RHSA) errata document security vulnerabilities in Red Hat products for which there are remediations or mitigations available. The Insights for Red Hat Enterprise Linux vulnerability service displays the advisory identifier tied to each system exposed to a CVE.

View this information by selecting a CVE and selecting the **Filter by affected systems** link in the security rule card. If an advisory exists for the system, the RHSA ID is visible as a link next to the system in the **Exposed systems** list, **Advisory** column. When there are no such advisories, the Advisory column is not visible, or will show “Not available.”

When an advisory exists for a system, users can view more information about the RHSA, including a list of affected systems. In the patch service, users can select systems to create an Ansible Playbook to apply the remediation.



2.2. SECURITY RULES

Security rules are CVEs given additional visibility due to the elevated risk and exposure associated with them. These are security flaws that may receive significant media coverage and have been scrutinized by the Red Hat Product Security team, using the Product Security Incident Response Plan workflow to help determine your RHEL environment exposure. These security rules enable you to take the appropriate action to protect your organization.

Security rules provide deep threat intelligence, beyond analyzing the version of RHEL running on a system. Security rules are manually curated to determine whether you are susceptible to a security threat by analyzing system metadata collected by the Insights client. If the vulnerability service identifies a system as exposed to a security rule, there is the potential for elevated security risk and issues should be addressed with urgency.

IMPORTANT

Addressing security rules on exposed systems should be your highest priority.

Finally, not all systems exposed to a CVE are also exposed to a security rule associated with that CVE. Even though you may be running a vulnerable version of software, other environmental conditions may mitigate the threat; for example, a specific port is closed or if you are running SELinux.

2.2.1. Identifying security rules in the Insights for RHEL dashboard

Use the following steps to view your infrastructure exposure to security rules.

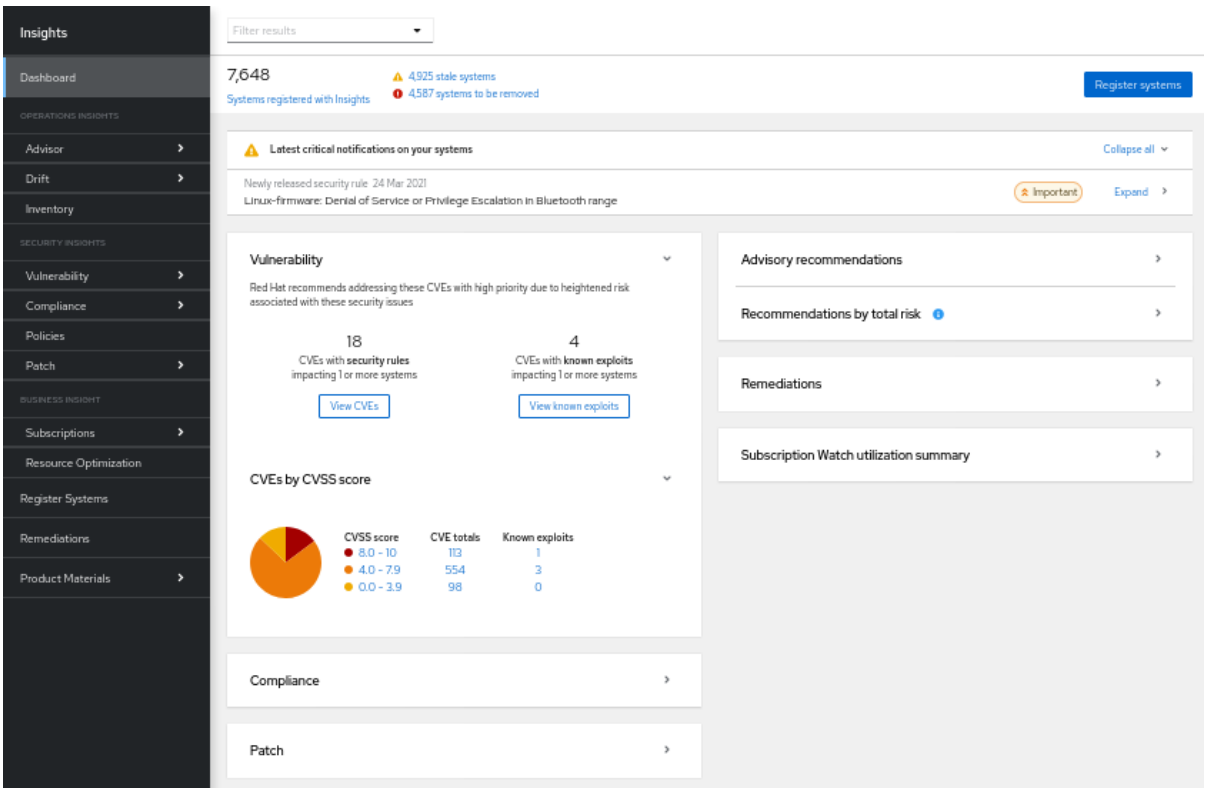
Procedure

1. Navigate to the Insights for Red Hat Enterprise Linux dashboard .

NOTE

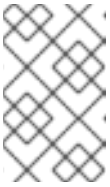
For simplicity, panels for services not related to security vulnerability assessment are minimized in the following screenshot.

:



2. View the **Latest critical notifications** on your systems panel. These are security rules with an elevated severity rating of “Important” or “Critical.” These are potentially your most critical issues and should be prioritized for remediation.

    a. To the right of each notification, click the **Expand** button to see associated CVEs and the number of systems exposed in your infrastructure.



NOTE

You may see security rules in your critical notifications but have zero systems exposed. In this case, even though the CVE is present in your infrastructure, the security rule conditions may not exist.

    b. Below the name of the security rule, and under Associated CVEs, click the CVE ID link.

    c. View which of your systems is impacted by the security rule CVE and optionally select exposed systems to create playbooks.

3. Next, view the information in the **vulnerability** card.

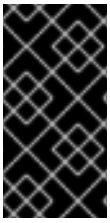
    a. Note the number of “CVEs with **security rules** impacting systems.” This number includes security rules of any severity impacting at least one system.

        i. Click **View CVEs**. Consider lesser-severity security rules your second highest priority for remediation, following high-severity security rules.

2.3. KNOWN EXPLOITS

Red Hat analyzes Metasploit data to determine whether code exists publicly to exploit a CVE, or a CVE has already been exploited publicly. The vulnerability service applies the “Known exploits” label to CVEs that meet that criteria.

This enhanced threat assessment can help users identify and address those CVEs that pose the most critical risks first. Red Hat recommends users review any CVEs with the “Known exploit” label with high priority and work towards remediating those issues.



IMPORTANT

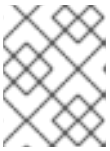
The vulnerability service makes you aware that the known-exploit CVE exists on systems in your infrastructure. The “Known exploits” label does not mean that the vulnerability was exploited on your RHEL systems; the vulnerability service does not make that determination.

2.3.1. Identifying known-exploit CVEs in the Insights for Red Hat Enterprise Linux dashboard

Use the following steps to identify known-exploit CVEs in the Insights for RHEL dashboard vulnerability card.

Procedure

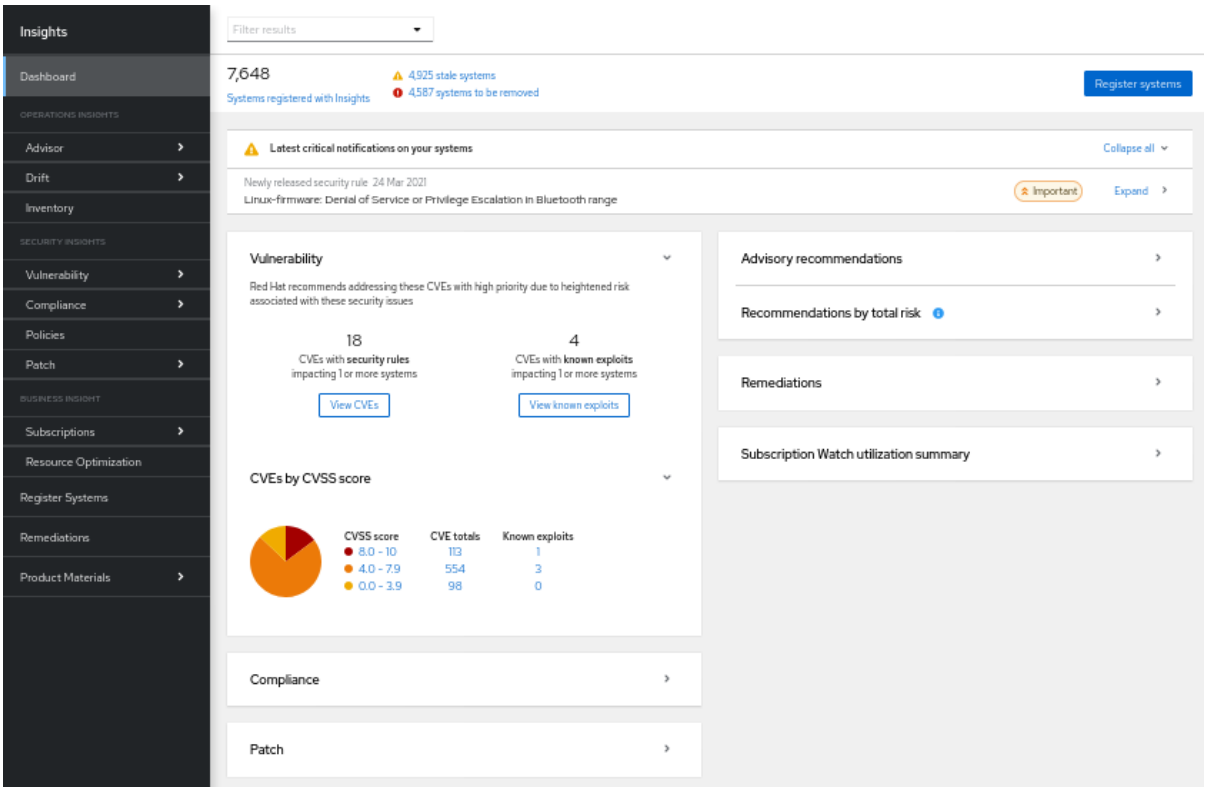
1. Navigate to the Insights for Red Hat Enterprise Linux dashboard .



NOTE

For simplicity, panels for services not related to security vulnerability assessment are minimized in the following screenshot.

:



2. On the **Vulnerability** card, note the **CVEs with known exploits impacting 1 or more systems and the number displayed**.

3. Click **View known exploits**.

4. View the filtered list of known-exploit CVEs in the CVEs list.

CHAPTER 3. REFINING VULNERABILITY SERVICE RESULTS

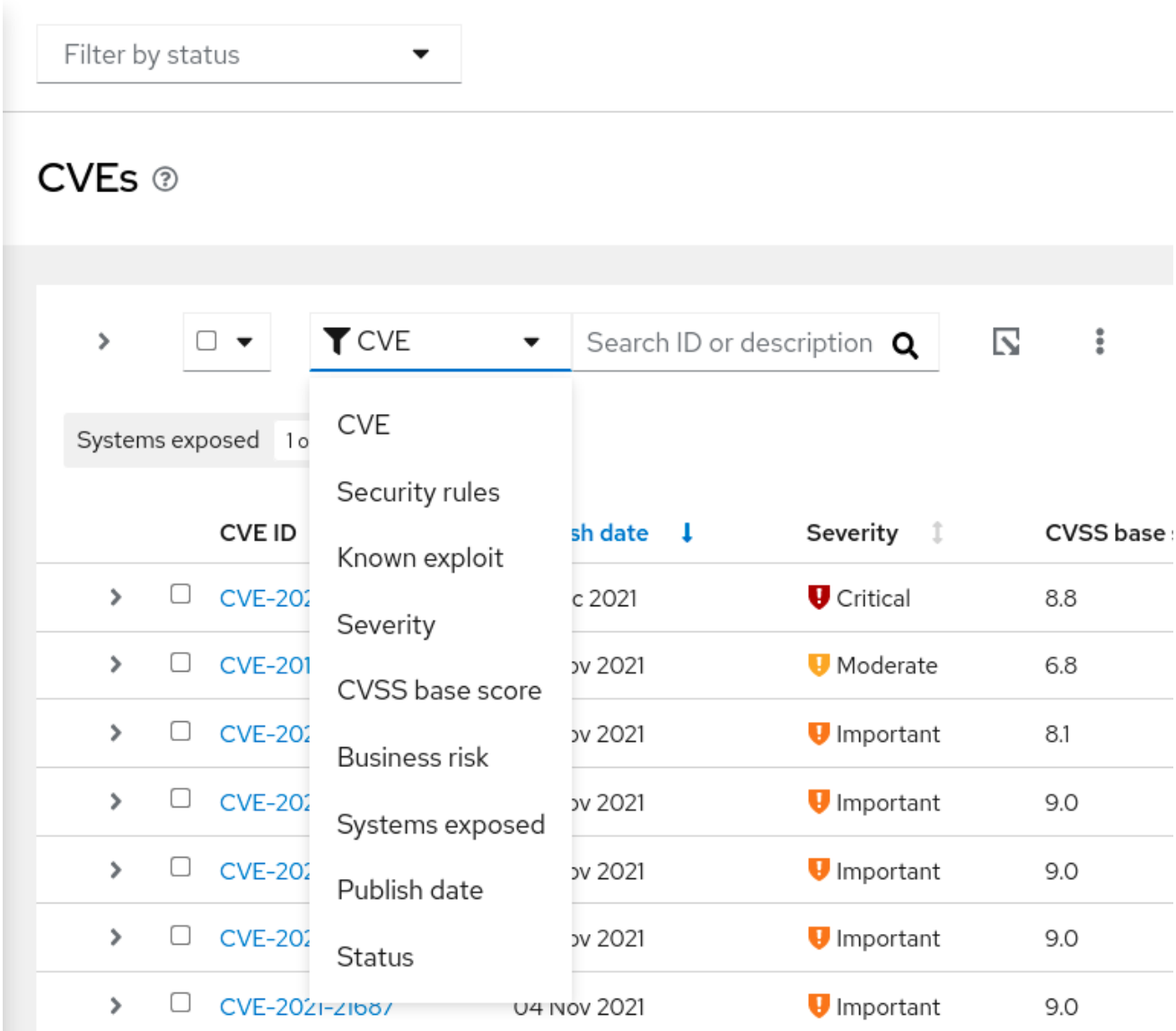
Whether reporting results to stakeholders or prioritizing systems for remediation, the vulnerability service enables many ways to refine the views of your data, helping you and others focus on your most critical systems, workloads, or issues. The following sections describe the organization of your data and the sorting, filtering, and contextual features you can use to refine and enrich your results.

3.1. CVE-LIST AND SYSTEMS-LIST FILTERS

Filtering narrows the visible list of CVEs and associated systems, helping you focus on specific issues. Apply filters to the CVEs list to focus on CVEs by criticality or business risk, for example. After selecting an individual CVE, apply filters to the resulting list of affected systems to focus on those of a specific RHEL major or minor version, for example.

Filters are activated by selecting a primary filter from the drop down list of filters on the left, and then selecting a secondary subfilter from the filter options drop down list on the right. Selected filters are visible below the Filters menu and can be deactivated by clicking the X next to each one.

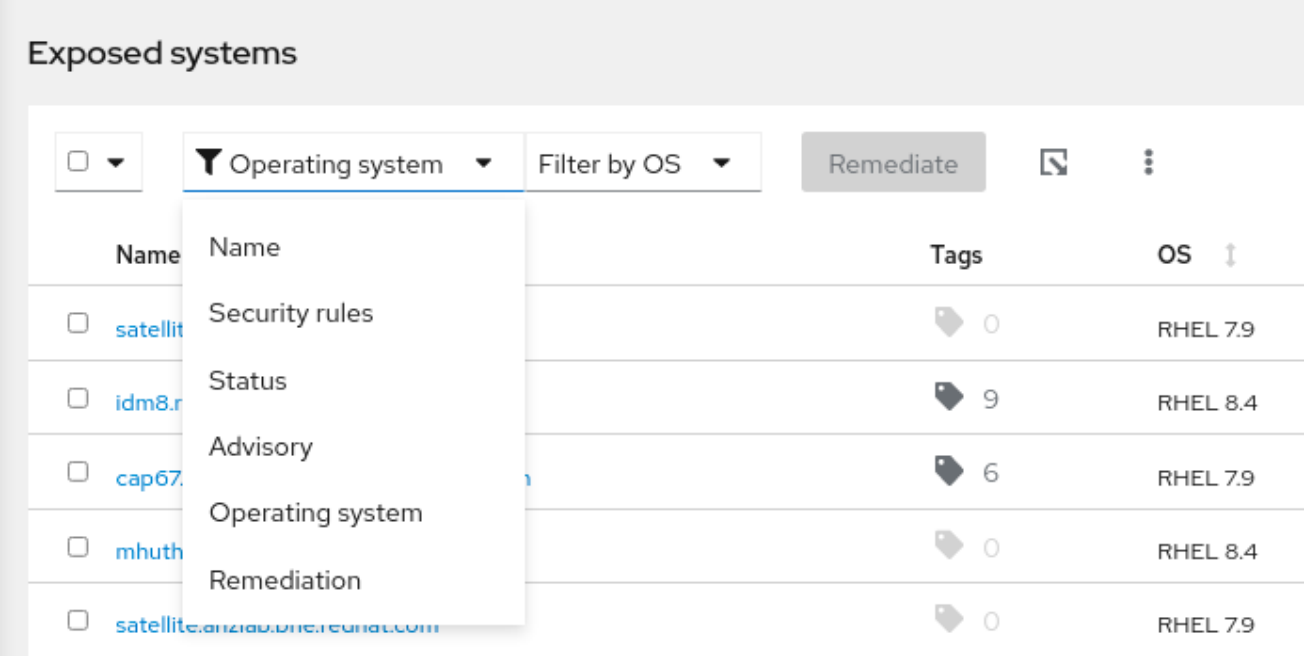
CVEs list filters



The following primary filters are accessible from the CVEs page. Select the primary filter, then define a parameter in the subfilter:

- **CVE.** Search ID or description.
- **Security rules.** Show only CVEs with the "Security rule" 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.
- **Systems exposed .** Select to only show CVEs with systems currently affected, or with no systems affected.
- **Publish date.** Select from All, Last 7 days, Last 30 days, Last 90 days, Last year, or More than 1 year ago.
- **Status.** Select one or more values: Not reviewed, In review, On-hold, Scheduled for patch, Resolved, No action - risk accepted, Resolved via mitigation.

Systems list filters



The following primary filters are accessible from the top of the list of systems on the CVE details page:

- **Name.** Find a specific CVE by entering the CVE ID.
- **Security rules.** If the CVE has a security rule associated with it, filter by other systems vulnerable to the same security rule, or show systems not affected by the security rule.
- **Status.** Show systems in specific status or workflow categories.
- **Advisory.** Show systems to which a Red Hat advisory applies for this CVE.
- **Operating system.** Show systems running specific RHEL (minor) versions.

- **Remediation.** Show systems included in an Ansible Playbook, a manual remediation, or that are not included in a current remediation plan.

3.1.1. Filtering security-rule CVEs

Security rules, especially high-severity security rules, pose the greatest potential threat to your infrastructure and should be considered the highest priority for identification and remediation. Use the following procedure to view only high-severity security-rule CVEs in the CVEs list and identify affected systems.

NOTE

Not all systems exposed to a CVE are also exposed to a security rule associated with that CVE. Even though you may be running a vulnerable version of software, other environmental conditions may mitigate the threat; for example, a specific port is closed or SELinux is enabled.

Procedure

1. Navigate to Red Hat Enterprise Linux > Vulnerability > CVEs in Insights for Red Hat Enterprise Linux.
2. Click the filters dropdown list in the toolbar.
   a. Apply the **Security rules** filter.
   b. Apply the **Has security rule** subfilter.
3. Scroll down to view security-rule CVEs. CVEs with security rules display the security-rule label located immediately below the CVE ID.

3.1.2. Filtering known-exploit CVEs

CVEs with the "Known exploit" label are determined by Red Hat to have exploits that exist in the wild; either the code exists publicly to exploit the CVE, or an exploit is known publicly to have already happened. For these reasons, known-exploit CVEs should be prioritized for identification and remediation.

IMPORTANT

Red Hat does not determine whether any of your registered systems have been exploited. We are simply identifying CVEs that may pose an extraordinary risk.

Use the following steps to filter known-exploit CVEs in the CVEs list:

Procedure

1. Navigate to Red Hat Enterprise Linux > Vulnerability > CVEs in Insights for Red Hat Enterprise Linux.
2. Click the filters drop-down list in the toolbar.
   a. Apply the **Known exploit** filter.
   b. Apply the **Has a known exploit** subfilter.

3. Scroll down to view the list of known-exploit CVEs.

3.1.3. Filtering lists of systems exposed to security rules

After filtering the list of CVEs to view only your most critical potential threats, select an individual CVE to view the list of exposed systems and apply a filter to the list.

Procedure

1. After selecting a security-rule CVE, scroll down to the **Exposed systems** list. Not every system in the list has the security rule conditions present for the CVE to be a security rule. Apply the following filter to see only the systems with security rule conditions present.
2. Select the **Security rules** filter from the primary filter dropdown list.
3. Check the **Has security rule** box in the secondary subfilter dropdown list.
4. View the systems with exposure to that CVE that also have the conditions present for the security rules.

3.2. INSIGHTS FOR RHEL GROUP FILTERS

The ability to filter vulnerability service results by groups of systems or workloads enables users to view only those systems tagged as belonging to a specific group. These can be systems running SAP workloads (or by SAP ID), by Satellite host groups, or by custom tags added to the Insights client configuration file.

Group filtering can be set globally in Insights for RHEL using the **Filter results** box located at the top of the page throughout the Insights for RHEL application. Group selection persists when changing from service to service and page to page. However, the functionality varies within the different Insights for RHEL services.

Group filtering works in the vulnerability Dashboard and vulnerability service CVEs and Systems lists.

Learn more about group tags and configuring custom tags in *Tags and system groups* section of this document.

3.2.1. Filtering Dashboard, CVEs, and Systems lists by group

Use the following procedure to filter vulnerability service CVE and Systems lists by group.

Procedure

1. Navigate to Red Hat Hybrid Cloud Console and log in.
2. Open the Insights for Red Hat Enterprise Linux application.
3. Click the down arrow on the **Filter results** box located at the top of any page in the Insights application.
4. Select a group by which to filter your systems.
   Search or scroll to view available tags. To browse the full list of available tags, scroll to the bottom of the list and click **View more**.

   Optionally,

a. Select SAP workloads.

b. Select systems by specific SAP IDs.

c. Select Satellite host collections.

d. Select systems identified by custom group tags.
To learn more about creating custom tags, see section, **Custom system tagging**, in this document.

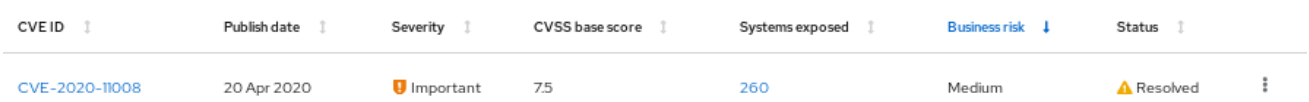
5. Navigate to the service and view only systems or CVEs that belong to your selected group or groups.

3.3. DEFINING A BUSINESS RISK FOR A CVE

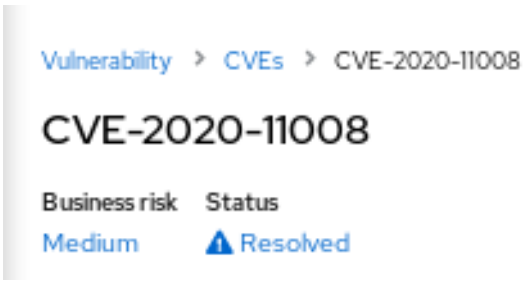
The vulnerability service allows you to define the business risk of a CVE with the following options: High, Medium, Low, or Not Defined (default).

While the list of CVEs shows the severity of each CVE, 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 Red Hat Enterprise Linux > Vulnerability > CVEs list, in the CVE row.

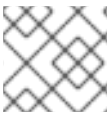


Business risk is also visible on the details card for each CVE, which shows more information and lists affected systems.



3.3.1. Setting a business risk for a single CVE

Complete the following steps to set the business risk for a single CVE:



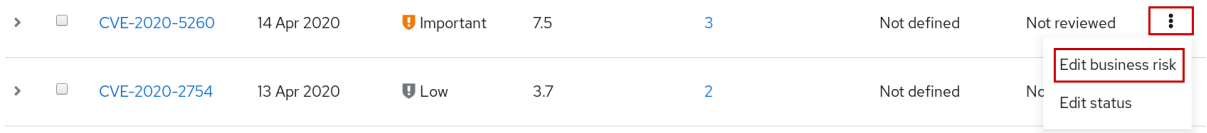
NOTE

The business risk for that CVE will be the same on *all* systems impacted by it.

1. Navigate to the Red Hat Enterprise Linux > Vulnerability > CVEs page and log in if necessary.

2. Identify a CVE for which to set a business risk.

3. Click the **more-actions** icon (three vertical dots) on the right end of the CVE row and click **Edit business risk**.



4. Set a business risk value to the appropriate level and, optionally, add a justification for your risk assessment.

5. Click **Save**.

3.3.2. Setting a business risk for multiple CVEs

Complete the following steps to set the same business risk on multiple CVEs that you select:

1. Navigate to Red Hat Enterprise Linux > Vulnerability > CVEs and log in if necessary.

2. Check the boxes for the CVEs for 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**.

3.4. 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 Insights for Red Hat Enterprise Linux services can still upload the data they need. It also means that you can still view results for those systems using filtering.

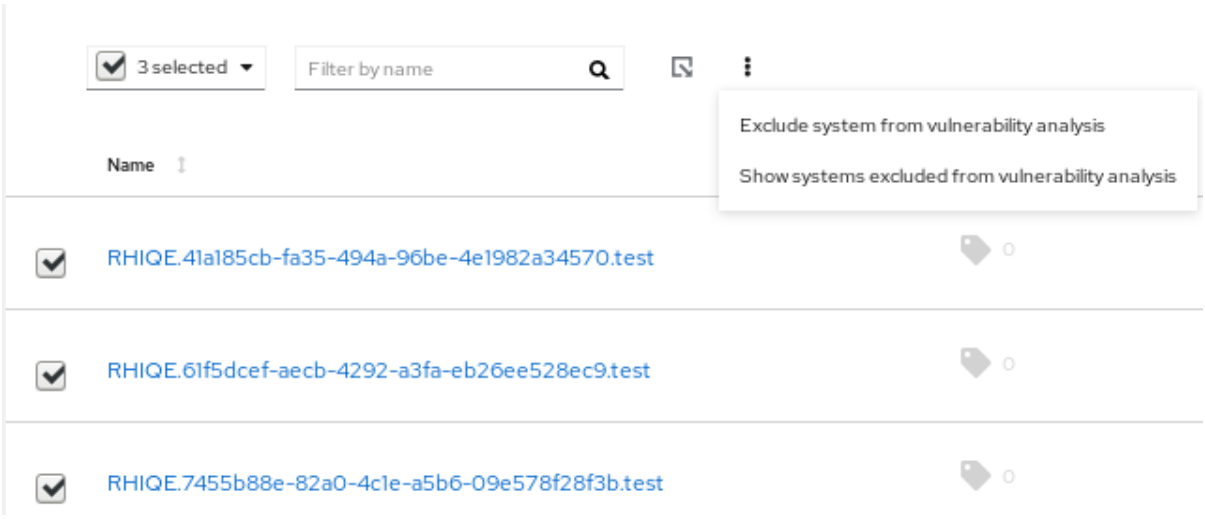
Complete the following steps to exclude selected RHEL systems from vulnerability service analysis:

Procedure

1. Navigate to the Red Hat Enterprise Linux > Vulnerability > 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. Optionally, you can exclude a *single* system by clicking the **more-actions** icon in the system row and selecting **Exclude system from vulnerability analysis**.

3.5. SHOWING PREVIOUSLY EXCLUDED SYSTEMS

Complete the following steps to show a previously excluded system:

Procedure

1. Navigate to the Red Hat Enterprise Linux > Vulnerability > 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 **Applicable CVEs** column.

3.6. RESUMING VULNERABILITY ANALYSIS FOR A SYSTEM

Complete the following steps to resume vulnerability analysis for a system:

Procedure

1. Navigate to the Red Hat Enterprise Linux > Vulnerability > 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**

3.7. CVE STATUS

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* .

Status values 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 facilitate better triaging through its life-cycle, from becoming aware of it to remediating it. Defining a status allows your organization to keep better tabs on where the most critical CVEs are in their life-cycle 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.

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

Complete the following steps 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 Red Hat Enterprise Linux > Vulnerability > 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**.

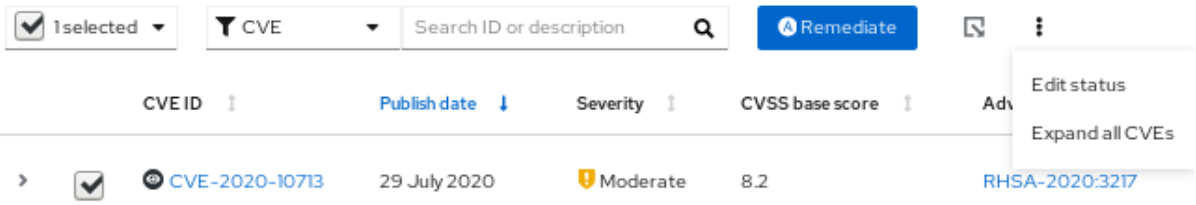
3.7.2. Setting a status for a CVE and system pair

Complete the following steps to set a status on a CVE and system pair:

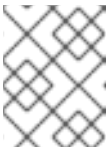
Procedure

1. Navigate to the Red Hat Enterprise Linux > Vulnerability > 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. Set a status for the CVE and system pair.



NOTE

If the box to **Use overall CVE status** is checked, you cannot set a status for the pair.

   b. Optionally, enter a justification for your status determination.
   c. Click **Save**.
6. Locate the CVE in the list and verify the status is set.

3.8. USING THE SEARCH BOX

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

- **CVEs page.** The search box is located in the toolbar at the top of the CVEs list. With the CVE filter set, search CVE IDs and descriptions.

- **Systems page.** The search box is located in the toolbar at the top of the list. Search for system name or UUID.

3.9. SORTING CVE LIST DATA

The sorting functions in the vulnerability service differ based on the context of the page you are viewing.

Procedure

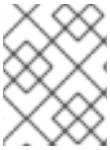
1. In the **CVEs tab**, you can apply sorting to the following columns:
   - CVE ID

- Publish date
- Severity
- CVSS base score
- Systems exposed
- Business risk
- Status

2. In the **Systems tab**, the following column can be sorted:
   - Name
   - Applicable CVEs
   - Last seen
3. After selecting a system in the Systems tab, the system-specific list of CVEs allows the following sorting options:
   - CVE ID
   - Publish date
   - Impact
   - CVSS base score
   - Business risk
   - Status

CHAPTER 4. SYSTEM TAGS AND GROUPS

Insights for Red Hat Enterprise Linux enables administrators to filter systems in inventory and in individual services using group tags. Groups are identified by the method of system data ingestion to Insights for RHEL. Insights for RHEL enables filtering groups of systems by those running SAP workloads, by Satellite host group, and by custom tags that are defined by system administrators with root access to configure the Insights client on the system.



NOTE

As of Fall 2020, the inventory, advisor, vulnerability, patch, drift, and policies services enable filtering by groups and tags. Other services will follow.

Use the global, **Filter results** dropdown to filter by SAP workloads, Satellite host groups, or custom tags added to the Insights client configuration file.

Prerequisites

The following prerequisites and conditions must be met to use the tagging features in Insights for Red Hat Enterprise Linux:

- The Insights client is installed and registered on each system.
- To create custom tags, root permissions, or their equivalent, are required to add to or change the **/etc/insights-client/tags.yaml** file.

4.1. SAP WORKLOADS

As Linux becomes the mandatory operating system for SAP ERP workloads in 2025, Red Hat Enterprise Linux and Insights for Red Hat Enterprise Linux are working to make Insights for RHEL the management tool of choice for SAP administrators.

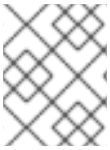
As part of this ongoing effort, Insights for RHEL automatically tags systems running SAP workloads and by SAP ID (SID), without any customization needed by administrators. Users can easily filter those workloads throughout the Insights for RHEL application by using the global **Search tags** dropdown menu.

4.2. SATELLITE HOST GROUPS

Satellite host groups are configured in Satellite and recognized automatically by Insights for Red Hat Enterprise Linux.

4.3. CUSTOM SYSTEM TAGGING

By applying custom grouping and tagging to your systems, you can add contextual markers to individual systems, filter by those tags in the Insights for Red Hat Enterprise Linux application, and more easily focus on related systems. This functionality can be especially valuable when deploying Insights for RHEL at scale, with many hundreds or thousands of systems under management.



NOTE

To create custom tags, root permissions, or their equivalent, are required to add to or change the **/etc/insights-client/tags.yaml** file.

4.3.1. Tag structure

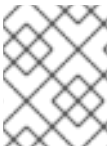
Tags use a **namespace/key=value** paired structure.

- **Namespace.** The namespace is the name of the ingestion point, *insights-client*, and cannot be changed. The **tags.yaml** file is abstracted from the namespace, which is injected by the client before upload.
- **Key.** The key can be a user-chosen key or a predefined key from the system. You can use a mix of capitalization, letters, numbers, symbols and whitespace.
- **Value.** Define your own descriptive string value. You can use a mix of capitalization, letters, numbers, symbols and whitespace.

4.3.2. The tags.yaml file

User-defined tags are added to the **/etc/insights-client/tags.yaml** file. You can add any number of key=value pairs to **tags.yaml**, as needed. The YAML syntax makes the contents easy to understand and modify.

Running **insights-client --group=eastern-sap** creates the tagging configuration file, **/etc/insights-client/tags.yaml** and adds the entry **group: eastern-sap**. The following example of a **tags.yaml** file shows additional tags added for the group "eastern-sap."



NOTE

You can use any mix of capitalization, letters, numbers, symbols, and whitespace when creating key=value pairs.

Example

```
# tags
---
group: eastern-sap
name: Jane Example
contact: jexample@corporate.com
Zone: eastern time zone
Location:
- gray_rack
- basement
Application: SAP
```

4.3.3. Creating a custom group and the tags.yaml file

Create and add tags to **/etc/insights-client/tags.yaml** simply by using **insights-client --group=<name-you-choose>**, which performs the following actions:

- Creates the **etc/insights-client/tags.yaml** file
- Adds the **group=** key and **<name-you-choose>** value to **tags.yaml**
- Uploads a fresh archive from the system to the Insights for Red Hat Enterprise Linux application so the new tag is immediately visible along with your latest results

After creating the initial **group** tag, add additional tags as needed by editing the **/etc/insights-client/tags.yaml** file.

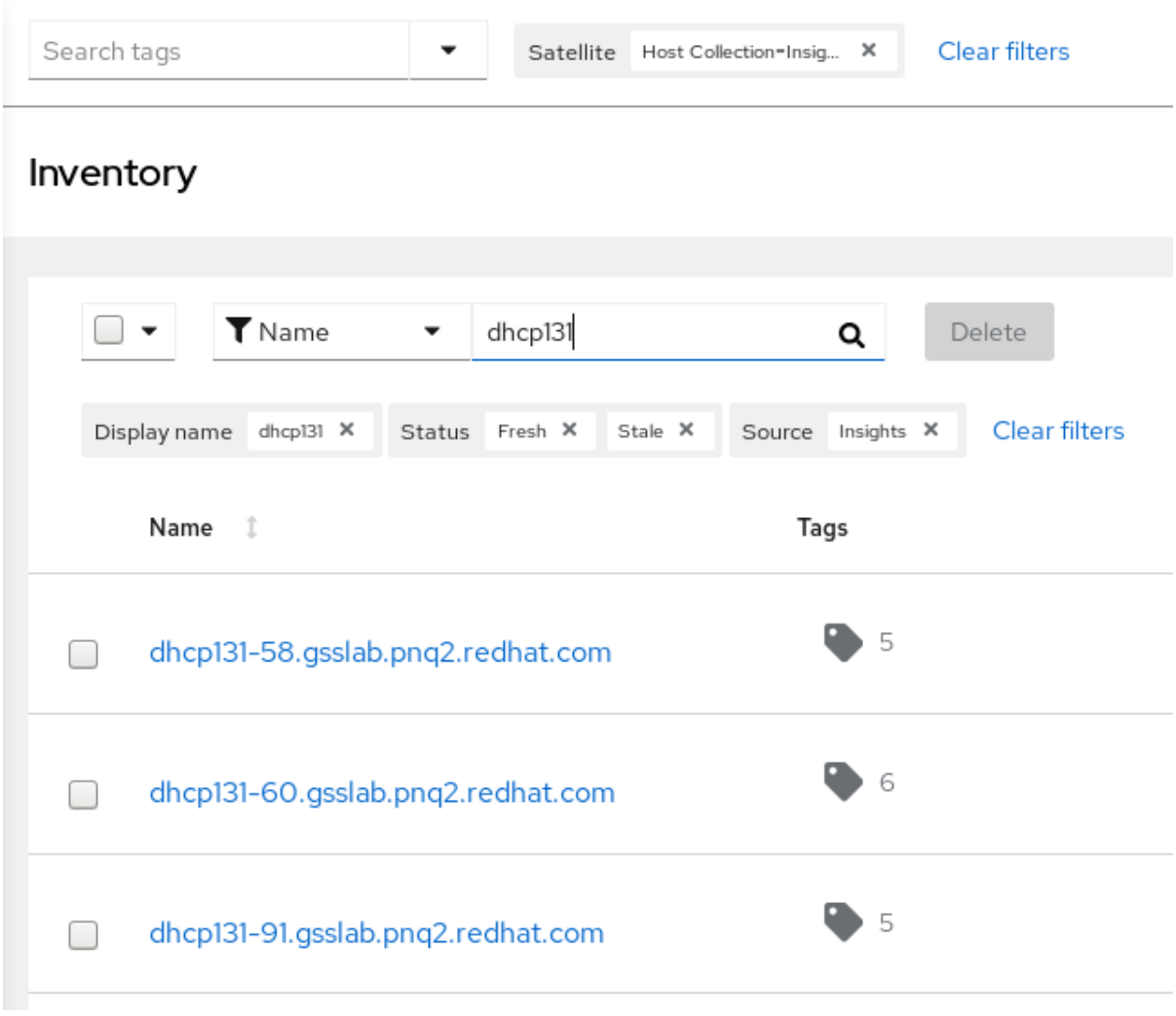
The following procedure shows how to create the initial group, as well as the **/etc/insights-client/tags.yaml** file, then verify the tag exists in the Insights for RHEL inventory.

Procedure

1. Run the following command as root, adding your custom group name after **--group=**:

```
[root@server ~]# insights-client --group=<name-you-choose>
```

2. Navigate to Red Hat Enterprise Linux > Inventory and log in if necessary.
3. Click the **Filter results** dropdown menu at the top of the page.
4. Scroll through the list or use the search function to locate specific tags.
5. Click the tag to filter by it.
6. Verify that your system is among the results on the vulnerability systems list.
7. Activate the **Name** filter and begin typing the system name until you see your system, then select it.
8. Verify that, next to the system name, the tag symbol is darkened and shows a number representing the correct number of tags applied.



4.3.4. Editing tags.yaml to add or change tags

After creating the group tag, edit the contents of **/etc/insights-client/tags.yaml** as needed to add or modify tags. You can add multiple, filterable tags to a system.

Procedure

1. Using the command line, open the tag configuration file for editing.
   [root@server ~]# vi /etc/insights-client/tags.yaml

2. Edit content or add additional values as needed. The following example shows how you can organize **tags.yaml** when adding multiple tags to a system.

```
# tags
---
group: eastern-sap
location: Boston
description:
- RHEL8
- SAP
key 4: value
```

NOTE

Add as many key=value pairs as you need. Use a mix of capitalization, letters, numbers, symbols, and whitespace.

3. Save your changes and close the editor.

4. Generate an upload to Insights for Red Hat Enterprise Linux.
   [root@server ~]# insights-client

5. Navigate to Red Hat Enterprise Linux > Inventory and log in if necessary.

6. In the **Filter results** dropdown at the top of the page, select tags or enter the name of the tag and select it.

7. Find your system among the results.

8. Verify that the tag icon is darkened and shows a number representing the number of tags applied to the system.

9. Click the tag to see each of the tags applied to that system.

CHAPTER 5. REFERENCE MATERIALS

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

- *Remediating Security Exposures using the Vulnerability Service and Ansible Playbooks*
- *Generating Vulnerability Service Reports*
- Insights for Red Hat Enterprise Linux Documentation
- Insights for Red Hat Enterprise Linux Product Support page