



# Red Hat Insights for OpenShift 1-latest

## Assessing security vulnerabilities in your OpenShift cluster using Red Hat Insights

Using Insights Vulnerability dashboard to assess cluster exposure to CVE vulnerabilities



# Red Hat Insights for OpenShift 1-latest Assessing security vulnerabilities in your OpenShift cluster using Red Hat Insights

---

Using Insights Vulnerability dashboard to assess cluster exposure to CVE vulnerabilities

## Legal Notice

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## Abstract

---

## Table of Contents

<b>CHAPTER 1. OVERVIEW OF RED HAT INSIGHTS FOR OPENSIFT VULNERABILITY DASHBOARD SERVICE</b>	<b>3</b>
1.1. ABOUT COMMON VULNERABILITIES AND EXPOSURES (CVES) IN VULNERABILITY DASHBOARD	3
1.2. DATA COLLECTION AND SECURITY	4
<b>CHAPTER 2. DETERMINING THE EXPOSURE OF YOUR OPENSIFT INFRASTRUCTURE TO CVES</b>	<b>5</b>
<b>CHAPTER 3. USING THE CVE LIST VIEW TO DETERMINE WHICH VULNERABILITIES AFFECT YOUR CLUSTER</b>	<b>6</b>
3.1. GETTING TO THE CVE LIST VIEW	6
3.2. REFINING THE CVE LIST VIEW RESULTS TO PROTECT YOUR ORGANIZATION	7
3.2.1. Searching for a specific CVE	7
3.2.2. Finding information about a specific CVE	8
3.2.3. Filtering results in the CVE list view	9
3.2.4. Filtering CVEs by severity	10
3.2.5. Sorting results in the CVE list view	11
3.3. ADDITIONAL RESOURCES	11
<b>CHAPTER 4. USING THE CLUSTERS LIST VIEW TO HELP YOU DETERMINE WHICH CLUSTERS ARE VULNERABLE TO CVES</b>	<b>12</b>
4.1. GETTING TO THE CLUSTERS LIST VIEW	12
4.2. REFINING THE CLUSTERS LIST VIEW RESULTS TO HELP PROTECT YOUR ORGANIZATION	12
4.2.1. Filtering results in the Clusters list view	13
4.2.2. Filtering clusters by CVE severity ratings	14
4.2.3. More information about filtering clusters by severity	14
4.2.3.1. CVE severity indicators	14
4.2.3.2. CVE severity filtering by context	15
4.2.4. Sorting cluster data	16
<b>CHAPTER 5. REFERENCE MATERIALS</b>	<b>17</b>



# CHAPTER 1. OVERVIEW OF RED HAT INSIGHTS FOR OPENSIFT VULNERABILITY DASHBOARD SERVICE

The Red Hat Insights for OpenShift Vulnerability dashboard service provides information about the exposure of your OpenShift cluster infrastructure to Common Vulnerabilities and Exposures (CVEs).

CVEs are security exposures or flaws identified in publicly-released software packages. Using the Vulnerability dashboard service, you can make assessments about, and perform comprehensive monitoring of, the exposure of your clusters to CVEs, enabling you to better understand, prioritize, and triage the highest risks posed to your organization. The Vulnerability dashboard provides CVE data for:

- Your OpenShift cluster infrastructure
- Some Red Hat products hosted on Red Hat marketplace

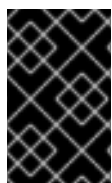


## NOTE

The Vulnerability dashboard service does not provide CVE data about the workloads that are running on the clusters.

You can interact with, triage, and assess the CVEs that might affect your clusters through

- a CVEs list view (shows a detailed view of CVEs, where you can view, sort, and filter to get more details about CVEs for affected clusters)
- a Clusters list view (shows a detailed view of vulnerable clusters, where you can view, sort, and filter to get more details about affected clusters)



## IMPORTANT

Red Hat does not determine whether any of your connected OpenShift clusters have been exploited. The Vulnerability dashboard service identifies CVEs that might pose a risk to clusters and images in your OpenShift Container Platform environment.

### Additional resources

- [Getting Started with Red Hat Insights Vulnerability for OpenShift](#)
- [Information about CVEs on mitre.org](#)

## 1.1. ABOUT COMMON VULNERABILITIES AND EXPOSURES (CVEs) IN VULNERABILITY DASHBOARD

You can use Vulnerability dashboard to identify Common Vulnerabilities and Exposures (CVEs) affecting your OpenShift clusters, and to help you understand the potential risks to your clusters.

You can use the visibility of CVEs affecting your OpenShift clusters to prioritize your most critical issues.



## IMPORTANT

Vulnerability dashboard does not contain every CVE included in the list of entries at <https://cve.mitre.org>. Only CVEs with Red Hat-issued security advisories (RHSAs) are included in Vulnerability dashboard.

### Additional resources

- [What is a CVE](#)
- [Information about CVEs at mitre.org](#)
- [Explaining Red Hat Errata](#)

## 1.2. DATA COLLECTION AND SECURITY

Red Hat Insights does not collect identifying information, such as user names, passwords, or certificates. See [Red Hat Insights Data & Application Security](#) for information about Red Hat Insights data collection and controls.

### Additional resources

- [About remote health monitoring](#)
- [Showing data collected by remote health monitoring](#)
- [Opting out of remote health reporting](#)



## CHAPTER 2. DETERMINING THE EXPOSURE OF YOUR OPENSIFT INFRASTRUCTURE TO CVES

The two primary starting points for determining the exposure of your OpenShift infrastructure to CVEs in the Red Hat Hybrid Cloud Console are:

- [Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs](#) , also referred to as CVEs list view. This view is your starting point for getting information about a CVE.
- [Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > Clusters](#) , also referred to as Clusters list view. This is your starting point for getting information about a cluster.

From the CVE and Cluster list views, you can navigate to two additional views,

- CVE details view
- Cluster details view

that offer more detailed information.



### NOTE

The names of these views are unwritten, and are used to provide a framework that helps guide you through navigating through the Insights Vulnerability information.

### What you can do in these views

In the four views,

- CVE list view
- CVE details view
- Cluster list view
- Cluster details view

you can view, filter, and sort information. Changing the way you view your results can help you triage and prioritize the exposure to your clusters. Here is a brief overview of the information you can use to better analyze your results:

- **CVE list view:** CVE ID, Publish date, Severity, CVSS score, Exposed clusters
- **CVE details view:** Name, Status, Version, Provider
- **Cluster list view:** Name, Status, Version, CVEs severity, Provider
- **Cluster details view:** CVE ID, Publish date, Severity, CVSS score

Later sections of this documentation discuss more detail about viewing, filtering, and sorting information in these views.

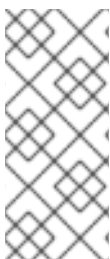
## CHAPTER 3. USING THE CVE LIST VIEW TO DETERMINE WHICH VULNERABILITIES AFFECT YOUR CLUSTER

In the CVE list view, you can triage the CVEs impacting your clusters so that you can take the appropriate actions to protect your organization. You can also focus on a single CVE by clicking on CVE ID to see details that help you understand exactly which clusters are exposed by that CVE.

In the default view of the CVE list view, you see:

- **CVE ID:** Shows details about the CVE, CVE ID number
- **Publish date:** Shows the date the CVE was published
- **Severity:** Shows the severity rating (Critical, Important, Moderate, Low, or Unknown) of the CVE
- **CVSS base score:** Shows the Common Vulnerability Scoring System (CVSS) base score 0-10)
- **Exposed clusters:** Shows the number of clusters currently affected

From this view, you can filter and sort using this criteria to help you focus on the most critical CVEs affecting your clusters.



### NOTE

The default view of the CVE list page shows a default filter selection (**Exposed clusters and 1 or More clusters**), which shows you those CVEs that affect one or more clusters in your organization. To see all CVEs, including those that do not affect any clusters reported by Vulnerability dashboard, you can click the **X** beside the filters to remove the filter.

### 3.1. GETTING TO THE CVE LIST VIEW

You can use Vulnerability dashboard to view CVEs affecting your organization to help you see information that helps you achieve your desired security posture.

#### Prerequisites

- Your Red Hat account and your cluster are registered to the same organization.
- Your account contains connected OpenShift clusters.
- You are logged into the Red Hat Hybrid Cloud Console.

#### Procedure

1. Navigate to the **Red Hat Hybrid Cloud Console**
2. Click **OpenShift**.
3. Click **Vulnerability**.
4. Click **CVEs**.

If you see a message that reads, “No CVEs found,” Red Hat Insights has not found any CVEs that affect your OpenShift infrastructure.

## 3.2. REFINING THE CVE LIST VIEW RESULTS TO PROTECT YOUR ORGANIZATION

To make the most use of Vulnerability dashboard, you can refine the CVE list view results by:

- [Searching for a specific CVE](#)
- [Finding information about a specific CVE](#)
- [Filtering results in the CVE list view](#)
- [Filtering CVEs by severity](#)
- [Sorting results in the CVE list view](#)

### 3.2.1. Searching for a specific CVE

If you know the CVE ID, you can use the filters in the CVE list view to search for details about that CVE.

#### Prerequisites

- Your Red Hat account and your cluster are registered within the same organization.
- Your account contains connected Red Hat-administered OpenShift clusters.
- You are logged into the Red Hat Hybrid Cloud Console.

#### Procedure

1. Navigate to [Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs](#) .
2. Select **CVE** in the filter drop-down list.
3. Enter or paste the CVE ID (for this example, *CVE-2022-2526*) into the search box.
4. Wait for the search results to populate (alternatively press Return or Enter). The search results show the **CVE ID**, **Publish date**, **Severity**, **CVSS base score**, and **Exposed clusters**.

5. Click the hyperlinked CVE ID for more details about the CVE and a list of affected clusters.

### 3.2.2. Finding information about a specific CVE

After locating a specific CVE, you can open the CVE details view. Here you will find the following additional information:

- CVE ID
- Publish date
- a brief description about the CVE
- Severity level
- CVSS base score
- a list of exposed clusters with the following sortable columns:
  - Name (name of the cluster)
  - Status
  - Type
  - Version
  - Provider
  - Last seen

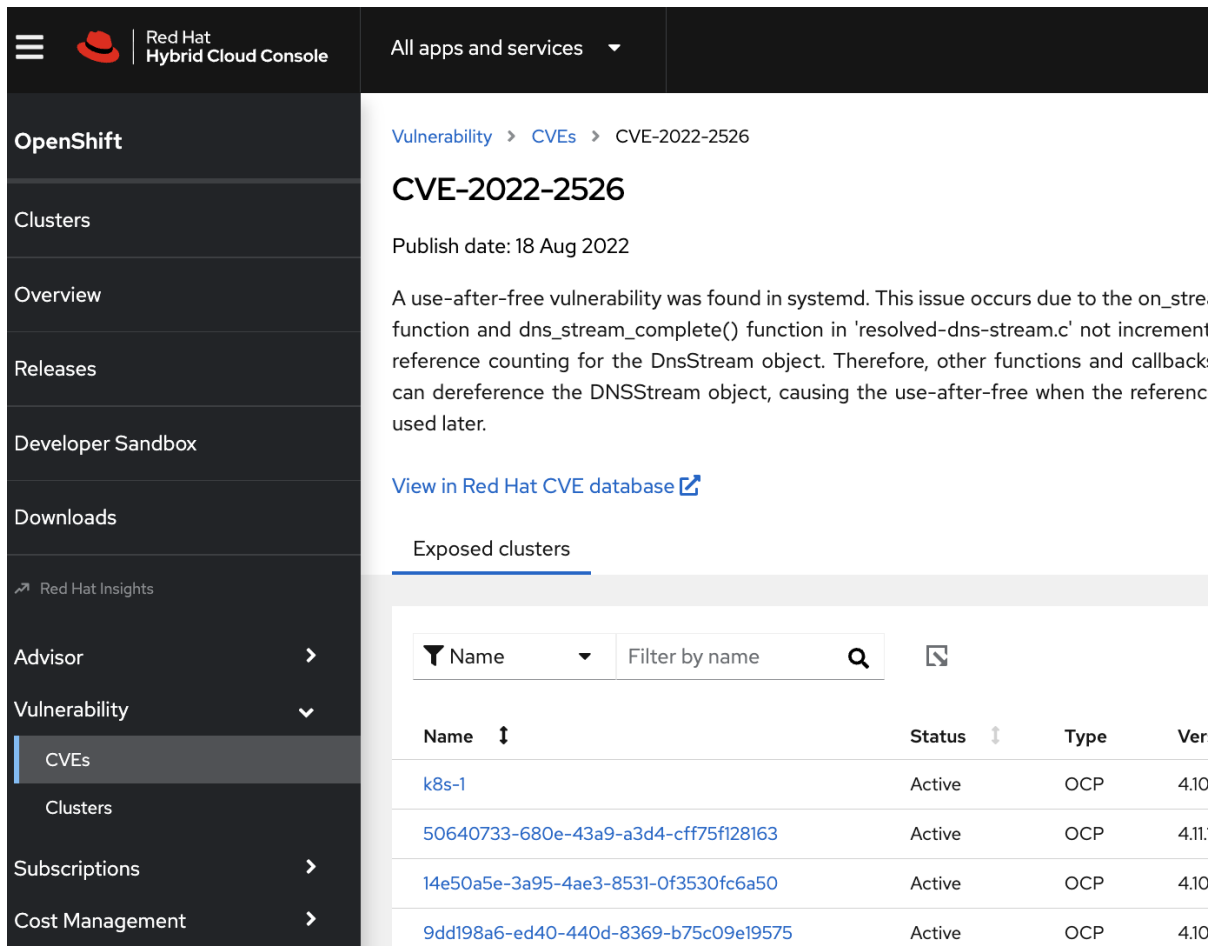
#### Prerequisites

- Your Red Hat account and your cluster are registered within the same organization.

- Your account contains connected Red Hat-administered OpenShift clusters.
- You are logged into the Red Hat Hybrid Cloud Console.

## Procedure

1. Navigate to [Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs](#)
2. Review the resulting list and find a CVE ID of interest (for example, 2022-2526).
3. Click the **CVE ID** in the CVE ID column. You see additional details about the CVE.



The screenshot shows the Red Hat Hybrid Cloud Console interface. On the left is a navigation sidebar with options like OpenShift, Clusters, Overview, Releases, Developer Sandbox, Downloads, Red Hat Insights, Advisor, Vulnerability, CVEs, Clusters, Subscriptions, and Cost Management. The main content area displays details for CVE-2022-2526, including its publish date (18 Aug 2022) and a description of a use-after-free vulnerability in systemd. Below the description is a link to view the CVE in the Red Hat CVE database. At the bottom, there is a section titled 'Exposed clusters' with a search filter and a table of clusters affected by the CVE.

Name	Status	Type	Ver
k8s-1	Active	OCP	4.10
50640733-680e-43a9-a3d4-cff75f128163	Active	OCP	4.11
14e50a5e-3a95-4ae3-8531-0f3530fc6a50	Active	OCP	4.10
9dd198a6-ed40-440d-8369-b75c09e19575	Active	OCP	4.10



## NOTE

If your clusters aren't affected by the CVE, you will see the message: "No matching clusters found."

### 3.2.3. Filtering results in the CVE list view

In the CVE list view, you can apply filters to the list of CVEs so that you can focus on specific information, such as the severity level of a CVE, or clusters in a specific version of OpenShift. After selecting an individual CVE, you can apply primary and secondary filters to the resulting list of clusters. The filters and options that you can apply are:

- **CVE ID:** Filter by ID or description.
- **Publish date:** Select from All, Last 7 days, Last 30 days, Last 90 days, Last year, or More than 1 year ago.

- **Severity:** Select one or more values: Critical, Important, Moderate, Low, or Unknown.
- **CVSS base score:** Enter a range from 0-10.
- **Exposed clusters:** Select to only show CVEs with clusters currently affected, or with no clusters affected.

### Prerequisites

- Your Red Hat account and your cluster are registered within the same organization.
- Your account contains connected OpenShift clusters.
- You are logged into the Red Hat Hybrid Cloud Console.

### Procedure

1. Navigate to [Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs](#)The default view of the CVE list view shows a default filter selection of **Exposed clusters**, and **1 or More clusters**.
2. Select a primary filter (for example, **Publish date**) from the drop-down list of filters on the left.
3. Select a secondary filter from the drop-down list of filters. For this example, select **Last 30 days** from the **Filter by publish date** drop-down arrow.



#### NOTE

The selected filters appear below the filter selection menu.

4. Confirm your filter selection, and then review the resulting information. This example shows CVEs from the last 30 days, if there are any.
5. To deactivate filters. click the **X** next to each filter (or any default filters) you selected, as needed.

If the last action results in a message indicating “No matching CVEs found,” this means your clusters are not affected by any CVEs.



#### NOTE

Filters remain active until you deselect them or leave the Vulnerability dashboard session. Reset or deselect unneeded filters to avoid unintended results.

### 3.2.4. Filtering CVEs by severity

In Vulnerability dashboard, you can filter the CVE list to show the most critical CVEs.

### Prerequisites

- Your Red Hat account and your cluster are registered within the same organization.
- Your account contains connected OpenShift clusters.
- You are logged into the Red Hat Hybrid Cloud Console.

## Procedure

1. Navigate to [Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs](#)
2. Click the drop-down filter list.
3. Select **Severity**.
4. Click the drop-down arrow in the **Filter by Severity** field.
5. Select a filter (for example, **Critical**) to display all CVEs with that severity rating.
6. Click the CVE ID to get additional information.

### 3.2.5. Sorting results in the CVE list view

You can also sort the list of CVEs in this view to triage the most relevant information first. For example, to see all of the most critical CVEs affecting your clusters, sort by the severity or CVSS base score. You can sort the CVE page results by these columns:

- CVE ID
- Publish date
- Severity
- CVSS base score
- Exposed clusters

## Prerequisites

- Your Red Hat account and your cluster are registered within the same organization.
- Your account contains connected OpenShift clusters.
- You are logged into the Red Hat Hybrid Cloud Console.

## Procedure

1. Navigate to [Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > CVEs](#)
2. Click the sort arrow next to the column you want to sort.

## 3.3. ADDITIONAL RESOURCES

- [Severity Ratings](#)
- [Official CVSS documentation](#)

## CHAPTER 4. USING THE CLUSTERS LIST VIEW TO HELP YOU DETERMINE WHICH CLUSTERS ARE VULNERABLE TO CVES

In the clusters list view, you can see the list of vulnerable clusters (also referred to as exposed clusters) in your organization. This view contains options you can choose to find information about a vulnerable cluster, view all the CVEs affecting the cluster and also all the clusters exposed to any of the resulting CVEs affecting the cluster.

The following information is shown at the top of the Clusters list view:

- **Name:** Shows the name of a vulnerable cluster that is affected by a CVE.
- **Status:** Shows the connection status (Connected, Stale, Not applicable or N/A of a cluster.
- **Version:** Shows the OpenShift Container Platform version (4.8+) of a cluster
- **CVEs severity:** Shows the severity level (Critical, Important, Moderate, Low) of the CVEs affecting the cluster.
- **Provider:** Shows the name of the cluster's cloud provider.
- **Last seen:** Shows the last time (in the form of minutes, hours, or days) since information was last uploaded from the cluster to the Vulnerability dashboard service.

### 4.1. GETTING TO THE CLUSTERS LIST VIEW

You can sort and filter information about your vulnerable clusters in the Clusters list view. Data in this view will help you focus on information that is important to your organization. To view data in the Clusters list view:

#### Prerequisites

- Your Red Hat account and your cluster are registered to the same organization.
- Your account contains connected OpenShift clusters.
- You are logged into the Red Hat Hybrid Cloud Console.

#### Procedure

1. Navigate to the **Red Hat Hybrid Cloud Console**
2. Click **OpenShift**.
3. Click **Vulnerability**.
4. Click **Clusters**.

### 4.2. REFINING THE CLUSTERS LIST VIEW RESULTS TO HELP PROTECT YOUR ORGANIZATION

To make the most use of Vulnerability dashboard, you can refine the Clusters list view results to:

- [Filter results in the Clusters list view](#)



- Filter clusters by CVE severity
- Sort cluster data

### 4.2.1. Filtering results in the Clusters list view

You can apply filters to a list of clusters in Vulnerability dashboard so that you can focus on specific information, such as the severity rating of a CVE, or clusters in a specific version of OpenShift Container Platform. After you select a CVE, you can apply filters to the resulting list of affected clusters.

The options for filtering in the Clusters list view are:

- **Name:** Filters on the name of a vulnerable cluster that is affected by a CVE.
- **Status:** Filters on the connection status (Connected, Disconnected, Stale, Not applicable or N/A) of a cluster.
- **Version:** Filters on the version (OpenShift Container Platform 4.8+) of a cluster.
- **CVEs severity:** Filters on the severity level (All clusters, Critical, Important, Moderate, Low) of the security-related issue and the number of images affected in the cluster.
- **Provider:** Filters on the name of the cluster's cloud provider.

#### Prerequisites

- Your Red Hat account and your cluster are registered within the same organization.
- Your account contains connected OpenShift clusters.
- You are logged into the Red Hat Hybrid Cloud Console.

#### Procedure

1. Navigate to [Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > Clusters](#)
2. Select a primary filter (for example, **CVEs severity**) from the drop-down list of filters on the left.
3. Select the secondary filter (for example, **Filter by CVEs severity**).
4. Select a severity rating (for example, **Critical**). The selected filters appear below the filter selection menu.
5. Review the resulting information. Clusters vulnerable to CVEs with a severity level of Critical show first in the list.



#### NOTE

The default view is *All clusters* which shows all clusters, even those not vulnerable to any CVE. Remove this filter if you want to only show clusters that are affected by at least one CVE reported by Vulnerability dashboard.

Filters remain active until you deselect them or leave an Vulnerability dashboard session. Reset or deselect unneeded filters to avoid unintended results. To deactivate filters, click the **X** next to each filter (or any default filters) that you selected.

## 4.2.2. Filtering clusters by CVE severity ratings

You can apply filters to a list of clusters in Vulnerability dashboard so that you can focus on information such as the severity level of a CVE. Red Hat applies severity ratings to CVEs using a four-point scale of Critical, Important, Moderate, and Low. You can use the ratings to help you take actions to protect your organization. Procedure modules should include the steps that users perform and address user motivation.

### Prerequisites

- Your Red Hat account and your cluster are registered within the same organization.
- Your account contains connected OpenShift clusters.
- You are logged into the Red Hat Hybrid Cloud Console.

### Procedure

1. Navigate to [Red Hat Hybrid Cloud Console > OpenShift > Vulnerability > Clusters](#)
2. Click the drop-down filter list.
3. Select the **CVEs severity** primary filter.
4. Click the **Filter by CVEs severity** secondary filter.
5. Deselect **All clusters**.
6. Select a severity level (for this example, select **Critical**). You will see a list of clusters that have CVEs rated with the severity level of the option you selected.
7. **(Optional)** Click any of the clusters shown in the **Name** column to obtain more information about a cluster.

## 4.2.3. More information about filtering clusters by severity

In Vulnerability dashboard, you can use the CVEs Severity filter to show clusters affected by CVEs with ratings of Critical, Important, Moderate, or Low. The default filter, **All clusters**, shows both vulnerable clusters with their CVE severity ratings, as well as clusters not vulnerable to CVEs.

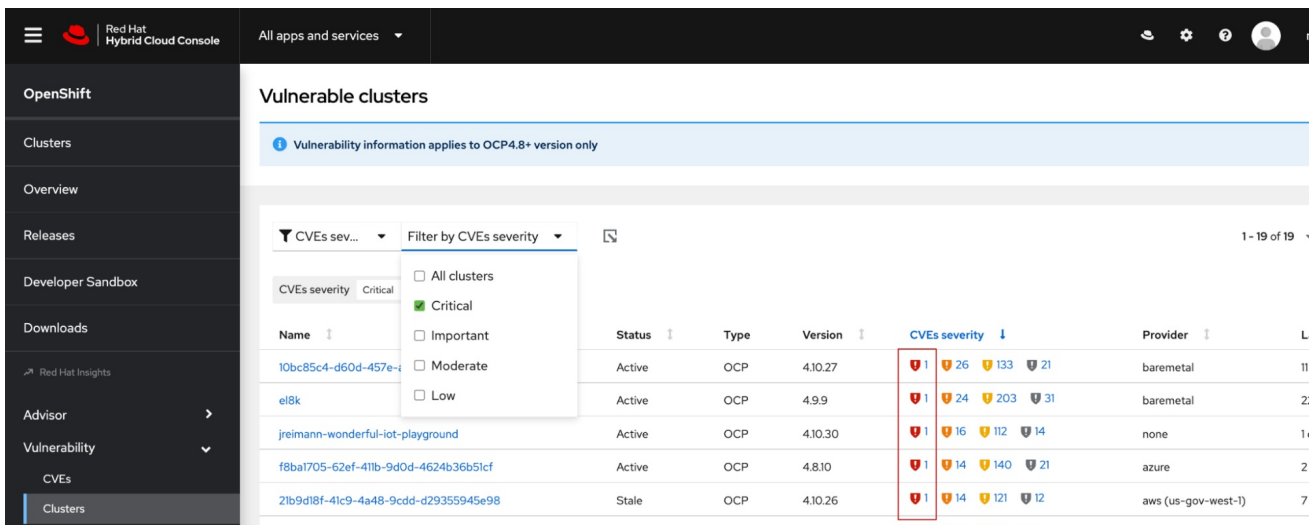
### 4.2.3.1. CVE severity indicators

Four icons represent the CVEs severity ratings from Critical to Low. The numbers beside the icons represent the respective number of CVEs with that severity type affecting that cluster. This representation allows you to quickly assess issue severity. The most critical issues will be displayed on the left with a color-coded red icon with an exclamation point in the middle. The icons represent increasingly lower severity rating levels when viewed from left to right.

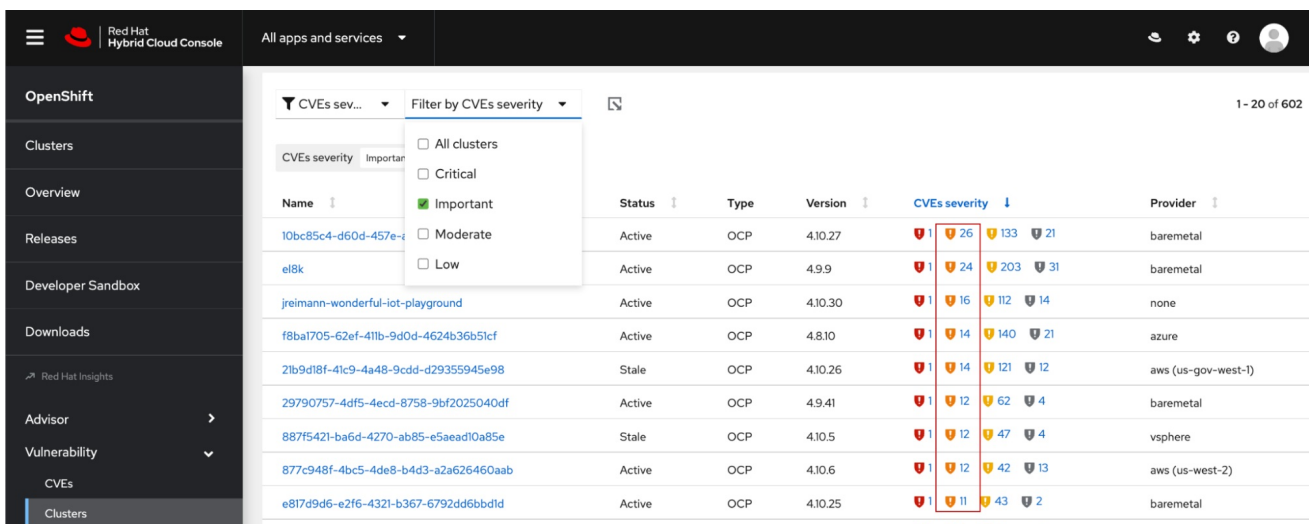


### 4.2.3.2. CVE severity filtering by context

The CVE severity ratings in the Clusters list view are filtered by context. Each filtered result is always shown in context of the most important, or higher-level rating. If you filter by the CVEs severity option of Critical you see a similar result as shown in the following image. This example shows several clusters affected by one critical CVE each.



If you change the filter to *Important*, you see that the top cluster has 26 CVEs with a severity level of Important. You also see any additional CVEs affecting the cluster as well as their severity levels. Note the Critical CVEs still showing in this filter by Important. Even though the cluster list is not filtered by the CVEs severity rating of Critical, the filter still takes into account the importance of the Critical severity, and shows the number of CVEs rated as Important along with the critical CVEs, as shown in the following image.



In this same filter session, results show a cluster with zero CVEs with a Critical severity rating, and 32 CVEs with a severity level of Important, as shown in the following image.

Clusters	23079f1b-cf48-4e05-a0ff-a35348cbebb8	Stale	OCP	4.10.12	🚩 1 🚩 10 🚩 43 🛡️ 1
Subscriptions >	5c73565a-a43d-47fa-8b27-cdd419a3a80d	Stale	OCP	4.10.12	🚩 1 🚩 10 🚩 43 🛡️ 1
Cost Management >	80963404-74b5-498e-babf-fc0f1372d151	Stale	OCP	4.11.0-rc.7	🚩 1 🚩 7 🚩 21 🛡️ 1
	aff5a913-lafa-4b0f-9dd3-f6ddef478f3	Active	OCP	4.10.6	🛡️ 0 🚩 32 🚩 178 🛡️ 25

Filtering in this context helps you see the most important information first.

#### 4.2.4. Sorting cluster data

In the Clusters list view, you can sort the following columns:

- **Name:** Shows the name of a vulnerable cluster that is affected by a CVE
- **Status:** Shows the connection status (Connected, Stale, Not applicable or N/A) of a cluster
- **Version:** Shows the OpenShift Container Platform version (4.8 or later) of a cluster.
- **CVEs severity:** Shows the severity level (Critical, Low, Moderate, Important) of the security-related issue and the number of images affected in the cluster.
- **Provider:** Shows the name of the cluster's cloud provider (AWS, Azure, etc.). This will vary as more cloud providers become available.

#### Additional Resources

- [Severity Ratings–Understanding Red Hat security ratings](#) .

## CHAPTER 5. REFERENCE MATERIALS

To learn more about the Red Hat Insights for OpenShift, see the following resources:

- [Red Hat Insights overview page](#)
- [Red Hat Insights Advisor for OpenShift](#)