



Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site



Red Hat F

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

RHSA

4-05-16

Overview

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

Updated In

Synop

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Importa

Type/

Security

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Topic

Red Hat
images t

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

ages and

This rele

Red Hat
Vulnerat

Common
ailable

Clearing your browser cookies may delete your cookie preferences. If you re-
for each vulnerability from the CVE link(s) in the References section.

Description

Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments.

This advisory contains the container images for Red Hat OpenShift Container Platform 4.12.57. See the following advisory for the RPM packages for this release:

<https://access.redhat.com/errata/RHSA-2024:2784>

Space precludes documenting all of the container images in this advisory. See the following Release Notes documentation, which will be updated shortly for this release, for details about these changes:

https://docs.openshift.com/container-platform/4.12/release_notes/ocp-4-12-release-notes.html

Security Fix(es):

- golang: net/http, x/net/http2: unlimited number of CONTINUATION frames

causes DoS (CVE-2023-45288)

- cluster-monitoring-operator: credentials leak (CVE-2024-1139)
- osin: manipulation of the argument secret leads to observable timing

discrepancy (CVE-2021-4294)

- ironic-image: Unauthenticated local access to Ironic API (CVE-2024-31463)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

All OpenShift Container Platform 4.12 users are advised to upgrade to these updated packages and images when they are available in the appropriate release channel. To check for available updates, use the OpenShift CLI (oc) or web console. Instructions for upgrading a cluster are available at <https://docs.openshift.com/container-platform/4.12/updating/updating-cluster-cli.html>

Solution

For OpenShift Container Platform 4.12 see the following documentation, which will be updated shortly for this release, for important instructions on how to upgrade your cluster and fully apply this asynchronous errata update:

https://docs.openshift.com/container-platform/4.12/release_notes/ocp-4-12-release-notes.html

You can download the oc tool and use it to inspect release image metadata for x86_64, s390x, ppc64le, and aarch64 architectures. The image digests can be found at

<https://quay.io/repository/openshift-release-dev/ocp-release?tab=tags>.

The sha values for the release are:

(For x86_64 architecture)

The image digest is

sha256:ebd20cd66e0bbb5bcd7d16559ff4856918b7172e29d6a7bd34d8cc49a556b8f7

(For s390x architecture)

The image digest is

sha256:7a18130347117b6c168a81a7311ba5eb74dcbaeafdb281d32d6a81254810d445

(For ppc64le architecture)


The image digest is

sha256:528a87f912c91861afa839b04b48fd6b8b79960d8872c8876c2de39821c74a39

(For aarch64 architecture)

The image digest is









sha256:0126ec3e0c154a2e8f45b92b8b41f8508d8a3c9ca096bb150c2bcc0740599b65

All OpenShift Container Platform 4.12 users are advised to upgrade to these updated packages and images when they are available in the appropriate release channel. To check for available updates, use the OpenShift CLI (oc) or web console. Instructions for upgrading a cluster are available at <https://docs.openshift.com/container-platform/4.12/updating/updating-cluster-cli.html> 

Affected Products

- Red Hat OpenShift Container Platform 4.12 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.12 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.12 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.12 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.12 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.12 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.12 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.12 for RHEL 8 aarch64

Fixes

- [BZ - 2156871](#)  - CVE-2021-4294 osin: manipulation of the argument secret leads to observable timing discrepancy
- [BZ - 2262158](#)  - CVE-2024-1139 cluster-monitoring-operator: credentials leak
- [BZ - 2268273](#)  - CVE-2023-45288 golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS
- [BZ - 2275847](#)  - CVE-2024-31463 ironic-image: Unauthenticated local access to Ironic API
- [OCPBUGS-30630](#)  - [4.12] BMH keep showing power status as off while IMM is powered on
- [OCPBUGS-31442](#)  - Dynamic irq load balancing issues
- [OCPBUGS-32429](#)  - [csi-snapshot-controller-operator] does not create suitable role and roleBinding for csi-snapshot-webhook
- [OCPBUGS-32449](#)  - multi-arch libvirt jobs need yq-v4

- [OCPBUGS-33253](#) - 4.12 Tracker: RIP: __list_del_entry_valid.cold - "ceph_drop_caps_for_unlink"

CVEs

- [CVE-2021-4294](#)
- [CVE-2021-25220](#)
- [CVE-2022-2795](#)
- [CVE-2022-3094](#)
- [CVE-2022-3204](#)
- [CVE-2022-24795](#)
- [CVE-2022-30698](#)
- [CVE-2022-30699](#)
- [CVE-2022-48624](#)
- [CVE-2023-4408](#)
- [CVE-2023-33460](#)
- [CVE-2023-45288](#)
- [CVE-2023-50387](#)
- [CVE-2023-50868](#)
- [CVE-2024-1139](#)
- [CVE-2024-1753](#)
- [CVE-2024-2357](#)
- [CVE-2024-2961](#)
- [CVE-2024-3154](#)
- [CVE-2024-28180](#)
- [CVE-2024-28834](#)
- [CVE-2024-31463](#)
- [CVE-2024-33599](#)
- [CVE-2024-33600](#)
- [CVE-2024-33601](#)
- [CVE-2024-33602](#)

References

- <https://access.redhat.com/security/updates/classification/#important>

The Red Hat security contact is secalert@redhat.com. More contact details at <https://access.redhat.com/security/team/contact/>.



Quick Links



Help



Site Info



Related Sites



✔ All systems operational



About Red Hat

Jobs

Events

Locations

Contact Red Hat

Red Hat Blog

Inclusion at Red Hat

Cool Stuff Store

Red Hat Summit

© 2026 Red Hat

Privacy statement

Terms of use

All policies and guidelines

Digital accessibility

Cookie Preferences and Opt-Out Rights