



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

5-02-27

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.

Importan

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
and ima

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

This rele

Red Hat
Vulnerab
for each

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser's global privacy

Common
ailable


Descri

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 4.16.36. See the following advisory for the RPM packages for this release:

<https://access.redhat.com/errata/RHBA-2025:1709>

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/4.16/release_notes/ocp-4-16-release-notes.html 

Security Fix(es):

- podman: buildah: Container breakout by using `--jobs=2` and a race


condition when building a malicious Containerfile (CVE-2024-11218)


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 4.16 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/4.16/updating/updating_a_cluster/updating-cluster-cli.html 

Solution

For OpenShift Container Platform 4.16 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/4.16/release_notes/ocp-4-16-release-notes.html 

You may download the `oc` tool and use it to inspect release image metadata for `x86_64`, `s390x`, `ppc64le`, and `aarch64` architectures. The image digests may be found at <https://quay.io/repository/openshift-release-dev/ocp-release?tab=tags>. 

The sha values for the release are as follows:

(For `x86_64` architecture)

The image digest is

sha256:efab0026a48c418ff01754238aea813e24097f65ff75962147cef78d785f06f4

(For `s390x` architecture)

The image digest is

sha256:0e508ce16974f094595ce3cef1f2b9c8c637eb4dfbbb7975b116197e1120fbcfb

(For `ppc64le` architecture)


The image digest is

sha256:f1cb4b67f7e23609c8e3871eb156949358fec43f031cb0a323240f43a67f3734

(For aarch64 architecture)

The image digest is











sha256:7a7711f2aa4ab7424522d44e65cce46e63fb15e8ab125547a099cd11a2e78acf

All OpenShift Container Platform 4.16 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/4.16/updating/updating_a_cluster/updating-cluster-cli.html 


Affected Products

- Red Hat OpenShift Container Platform 4.16 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform for Power 4.16 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.16 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.16 for RHEL 9 aarch64

Fixes

- [BZ - 2326231](#)  - CVE-2024-11218 podman: buildah: Container breakout by using --jobs=2 and a race condition when building a malicious Containerfile
- [OCPBUGS-35394](#)  - Fix console server's sessions pruning
- [OCPBUGS-43469](#)  - Azure Session for Client Certificate Credential Should Set Options to Send Certificate Chain
- [OCPBUGS-43680](#)  - rendered MachineConfig in use not recreated in OpenShift 4.16
- [OCPBUGS-46493](#)  - SDN Pods consume too much RAM during OVN Live migration, It caused the migration failure in OCP with 500 worker nodes
- [OCPBUGS-48082](#)  - [4.16] Update must-gather owners (artificial PR for backports)
- [OCPBUGS-48762](#)  - [4.16] Bootimage bump tracker
- [OCPBUGS-50575](#)  - [release-4.16] Increase waitForFallbackDegradedConditionTimeout of test e2e-sno-disruptive
- [OCPBUGS-50627](#)  - [4.16] Unable to configure nodeSelector and toleration for nmstate-console-plugin
- [OCPBUGS-50862](#)  - MCO doesn't recover pool from degraded state



CVEs


- [CVE-2024-11218](#) 


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 

 Loading



[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](#)