RHSA-2024:10528 - Security Advisory

Issued: 2024-12-04 Updated: 2024-12-04

Overview

Updated Images

Synopsis

Important: OpenShift Container Platform 4.16.25 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.16.25 is now available with updates to packages and images that fix several bugs and add enhancements.

This release includes a security update for Red Hat OpenShift Container Platform 4.16.

Red Hat Product Security has rated this update as having a security impact of important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available 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 4.16.25. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHBA-2024:10531

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):

- pam: Improper Hostname Interpretation in pam_access Leads to Access

Control Bypass (CVE-2024-10963)

- QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server

During Socket Closure (CVE-2024-7409)

- microcode_ctl: Denial of Service (CVE-2024-24968)

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
sha256:6be262c95acd928771f39e50afc7f1a628d5e20a2ba8c9a83a176c8eff809c06

(For s390x architecture)
The image digest is
sha256:d5fade25cc327a0f1b2174e9588ade616e4c240434e6a5e86088a2e5e9073431

(For ppc64le architecture)
The image digest is
sha256:8404b9ab00ca563e234145c0c7ab8f23600ad768639c5d28b56efec709db95eb

(For aarch64 architecture)
The image digest is
sha256:284e30f29de4ca6220aadc4a691045d61b324308e51e3d5ddaf71d82bce8e816

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 - 2302487 - CVE-2024-7409 QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server During Socket Closure
- BZ - 2312594 - CVE-2024-24968 microcode_ctl: Denial of Service
- BZ - 2324291 - CVE-2024-10963 pam: Improper Hostname Interpretation in pam_access Leads to Access Control Bypass
- OCPBUGS-31416 - Support envfrom on Operator Lifecycle Manager
- OCPBUGS-42727 - Live migration: CNO should report as a metric when there is network overlap
- OCPBUGS-43447 - Env vars mentioned in Func.yaml not rendered in the Env section of the Import Forms
- OCPBUGS-43930 - OLM Catalog ImageStreams not getting updated on minor release upgrade
- OCPBUGS-44207 - Create RoleBinding will trigger Admission Webhook Warning
- OCPBUGS-44348 - [release-4.16] ABI cluster installation fails for external OCI platform
- OCPBUGS-44846 - [release-4.16] Provide support for user owned IPsec machine configs
- OCPBUGS-44885 - [release-4.17] Silenced alert seen on openshift console overview page

- OCPBUGS-44932 - add IBM Block Storage CSI driver support for RWX

CVEs

- CVE-2022-48804
- CVE-2023-52619
- CVE-2023-52635
- CVE-2023-52775
- CVE-2023-52811
- CVE-2024-7409
- CVE-2024-10963
- CVE-2024-24968
- CVE-2024-26601
- CVE-2024-26615
- CVE-2024-26686
- CVE-2024-26704
- CVE-2024-27399
- CVE-2024-36960
- CVE-2024-38384
- CVE-2024-38541
- CVE-2024-38555
- CVE-2024-39507
- CVE-2024-40997
- CVE-2024-41007
- CVE-2024-41008
- CVE-2024-41009
- CVE-2024-41031
- CVE-2024-41038
- CVE-2024-41056
- CVE-2024-41093
- CVE-2024-42154
- CVE-2024-42228
- CVE-2024-42237
- CVE-2024-42238
- CVE-2024-42240
- CVE-2024-42241
- CVE-2024-42243
- CVE-2024-42244
- CVE-2024-42271
- CVE-2024-44309
- CVE-2024-44989

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/.

Red Hat

Quick Links

Help

Site Info

Related Sites

Partial system outage

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