RHSA-2024:6687 - Security Advisory

Issued: 2024-09-19 Updated: 2024-09-19

Synopsis

Important: OpenShift Container Platform 4.16.13 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.16.13 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 4.16.13.

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):

- openshift/builder: Path traversal allows command injection in privileged

BuildContainer using docker build strategy (CVE-2024-7387)

- openshift-controller-manager: Elevated Build Pods Can Lead to Node

Compromise in OpenShift (CVE-2024-45496)

- jose-go: improper handling of highly compressed data (CVE-2024-28180)

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.

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

(For x86_64 architecture)
The image digest is
sha256:6078cb4ae197b5b0c526910363b8aff540343bfac62ecb1ead9e068d541da27b

(For s390x architecture)
The image digest is
sha256:5b286b07b5267aa96af112f6420444d91c529456b7dc7e15d49ab4ef89ca9713

(For ppc64le architecture)
The image digest is
sha256:6c6b61c7890d49346e653b117c46f74171b2a65ce18edf11afa331e115ff392d

(For aarch64 architecture)
The image digest is
sha256:9d2928127d6a440a8931b4a0c6f565cb490338804e920f4493fb7ce875884baa

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 - 2268854 - CVE-2024-28180 jose-go: improper handling of highly compressed data
- BZ - 2302259 - CVE-2024-7387 openshift/builder: Path traversal allows command injection in privileged BuildContainer using docker build strategy
- BZ - 2308661 - CVE-2024-45496 openshift-controller-manager: Elevated Build Pods Can Lead to Node Compromise in OpenShift

CVEs

- CVE-2024-7387
- CVE-2024-28180
- CVE-2024-38428
- CVE-2024-45496

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

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

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility