RHSA-2024:10813 - Security Advisory

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

Synopsis

Important: OpenShift Container Platform 4.13.54 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.13.54 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 4.13.

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

https://access.redhat.com/errata/RHSA-2024:10815

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/4.13/release_notes/ocp-4-13-release-notes.html

Security Fix(es):

- golang: net/http, x/net/http2: rapid stream resets can cause excessive

work (CVE-2023-44487) (CVE-2023-39325)

- openshift-console: OAuth2 insufficient state parameter entropy

(CVE-2024-6508)

- golang-github-gin-gonic-gin: Improper Input Validation (CVE-2023-26125)
- QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server

During Socket Closure (CVE-2024-7409)

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 4.13 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/4.13/updating/updating_a_cluster/updating-cluster-cli.html

Solution

For OpenShift Container Platform 4.13 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/4.13/release_notes/ocp-4-13-release-notes.html

You may download the oc tool and use it to inspect release image metadata for x86_64 architecture. 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:bfe066b4b30eeb48f1099339131d56d4005f0867d4e4b3484e3fcfee39b3d26f

All OpenShift Container Platform 4.13 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/4.13/updating/updating_a_cluster/updating-cluster-cli.html

Affected Products

- Red Hat OpenShift Container Platform 4.13 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.13 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.13 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.13 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 8 aarch64

Fixes

- BZ - 2203769 - CVE-2023-26125 golang-github-gin-gonic-gin: Improper Input Validation
- BZ - 2243296 - CVE-2023-39325 golang: net/http, x/net/http2: rapid stream resets can cause excessive work (CVE-2023-44487)
- BZ - 2295777 - CVE-2024-6508 openshift-console: OAuth2 insufficient state parameter entropy
- BZ - 2302487 - CVE-2024-7409 QEMU: Denial of Service via Improper Synchronization in QEMU NBD Server During Socket Closure
- OCPBUGS-42951 - The filepath including leading slash makes error during parsing devfile using Gitlab
- OCPBUGS-43886 - Load Red Hat keys in FIPS mode with Go 1.22
- OCPBUGS-44206 - Panic seen in CI job for MCC pod
- OCPBUGS-44585 - Need to allow blank for Project/namespace when setting SA Subject in 'Project access tab'
- OCPBUGS-44692 - ClusterResourceOverride Operator creating high quantity of clusterresourceoverride-token secrets (57k) in the OCP cluster

CVEs

- CVE-2023-0597
- CVE-2023-26125
- CVE-2023-39325
- CVE-2023-52522
- CVE-2023-52619
- CVE-2023-52749

- CVE-2023-52881
- CVE-2024-6508
- CVE-2024-7409
- CVE-2024-26640
- CVE-2024-26656
- CVE-2024-26772
- CVE-2024-26870
- CVE-2024-26906
- CVE-2024-26984
- CVE-2024-27399
- CVE-2024-31076
- CVE-2024-36920
- CVE-2024-36928
- CVE-2024-37356
- CVE-2024-38796
- CVE-2024-40931
- CVE-2024-40988
- CVE-2024-41009
- CVE-2024-41014
- CVE-2024-41039
- CVE-2024-41041
- CVE-2024-41093
- CVE-2024-42154
- CVE-2024-42240
- CVE-2024-42271
- CVE-2024-43854
- CVE-2024-46858
- CVE-2024-49768
- CVE-2024-49769

References

- https://access.redhat.com/security/updates/classification/#important
- https://access.redhat.com/security/vulnerabilities/RHSB-2023-003

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