RHSA-2024:5200 - Security Advisory

Issued: 2024-08-19 Updated: 2024-08-19

Synopsis

Important: OpenShift Container Platform 4.12.63 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.12.63 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 4.12.

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

https://access.redhat.com/errata/RHSA-2024:5202

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):

- openshift/telemeter: iss check during JWT authentication can be bypassed

(CVE-2024-5037)

- kernel: net: kernel: UAF in network route management (CVE-2024-36971)
- ssh: Prefix truncation attack on Binary Packet Protocol (BPP)

(CVE-2023-48795)

- go-retryablehttp: url might write sensitive information to log file

(CVE-2024-6104)

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 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
sha256:5db6f8dd1db6b9d07dacfa74574a38a6e518145a3c0ab5d895e9c89e029a39e4

(For s390x architecture)
The image digest is
sha256:98c249ae7bbcb1824f1e500cce47cf4639e25341006d17c088051ceea0f96c28

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 - 2254210 - CVE-2023-48795 ssh: Prefix truncation attack on Binary Packet Protocol (BPP)
- BZ - 2272339 - CVE-2024-5037 openshift/telemeter: iss check during JWT authentication can be bypassed
- BZ - 2292331 - CVE-2024-36971 kernel: net: CVE-2024-36971 kernel: UAF in network route management
- BZ - 2294000 - CVE-2024-6104 go-retryablehttp: url might write sensitive information to log file
- OCPBUGS-37422 - Resolve snyk issue: k8s.io/client-go/transport [4.12]

CVEs

- CVE-2023-45290
- CVE-2023-48795
- CVE-2024-5037
- CVE-2024-6104
- CVE-2024-6345
- CVE-2024-6409
- CVE-2024-24790
- CVE-2024-34064
- CVE-2024-35235

- CVE-2024-36971
- CVE-2024-37298
- CVE-2024-37891
- CVE-2024-38428
- CVE-2024-38473
- CVE-2024-39331
- CVE-2024-39573

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/.