RHSA-2025:2441 - Security Advisory

Issued: 2025-03-13 Updated: 2025-03-13

Overview

Updated Images

Synopsis

Important: OpenShift Container Platform 4.12.74 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.12.74 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 4.12.74. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2025:2443

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):

- bind: bind9: Many records in the additional section cause CPU exhaustion

(CVE-2024-11187)

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

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

- runc: file descriptor leak (CVE-2024-21626)
- golang.org/x/net/html: Non-linear parsing of case-insensitive content in

golang.org/x/net/html (CVE-2024-45338)

- kernel: HID: core: zero-initialize the report buffer (CVE-2024-50302)

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 architectures. The image digests may be found at https://quay.io/repository/openshift-release-dev/ocp-release?tab=tags.

The sha value for the release is as follows:

(For x86_64 architecture)
The image digest is
sha256:7257adeedec4ace7a71d419c154855773219af4183eff625c716d0923230220f

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 - 2258725 - CVE-2024-21626 runc: file descriptor leak
- BZ - 2326231 - CVE-2024-11218 podman: buildah: Container breakout by using --jobs=2 and a race condition when building a malicious Containerfile
- BZ - 2327169 - CVE-2024-50302 kernel: HID: core: zero-initialize the report buffer
- BZ - 2333122 - CVE-2024-45338 golang.org/x/net/html: Non-linear parsing of case-insensitive content in golang.org/x/net/html
- BZ - 2342879 - CVE-2024-11187 bind: bind9: Many records in the additional section cause CPU exhaustion
- OCPBUGS-48086 - [4.12] Update must-gather owners (artificial PR for backports)
- OCPBUGS-49644 - OWNERS update
- OCPBUGS-50880 - [release-4.12] Increase waitForFallbackDegradedConditionTimeout of test e2e-sno-disruptive

CVEs

- CVE-2020-11023
- CVE-2023-52922
- CVE-2024-11187
- CVE-2024-11218
- CVE-2024-21626
- CVE-2024-45338
- CVE-2024-50302
- CVE-2024-53197
- CVE-2025-1094
- CVE-2025-1244

References

- https://access.redhat.com/security/updates/classification/#important
- https://access.redhat.com/security/vulnerabilities/RHSB-2024-001

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.

Cool Stuff Store

Red Hat Summit
