RHSA-2025:2701 - Security Advisory

Issued: 2025-03-20 Updated: 2025-03-20

Synopsis

Important: OpenShift Container Platform 4.13.56 bug fix and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat OpenShift Container Platform release 4.13.56 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 4.13.56. See the following advisory for the RPM packages for this release:

https://access.redhat.com/errata/RHSA-2025:2703

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.redhat.com/en/documentation/openshift_container_platform/4.13/html/release_notes

Security Fix(es):

- buildah: Buildah allows arbitrary directory mount (CVE-2024-9675)
- podman: buildah: Container breakout by using --jobs=2 and a race

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

- rsync: Info Leak via Uninitialized Stack Contents (CVE-2024-12085)
- 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: media: uvcvideo: Skip parsing frames of type UVC_VS_UNDEFINED in

uvc_parse_format (CVE-2024-53104)

- kernel: ALSA: usb-audio: Fix potential out-of-bound accesses for Extigy

and Mbox devices (CVE-2024-53197)

- libxml2: Use-After-Free in libxml2 (CVE-2024-56171)
- 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 4.13 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.redhat.com/en/documentation/openshift_container_platform/4.13/html-single/updating_clusters/index#updating-cluster-within-minor.

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.redhat.com/en/documentation/openshift_container_platform/4.13/html/release_notes

You may download the oc tool and use it to inspect release image metadata for the x86_64 architecture. 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
sha256:1b45fabb8dc896cdf904ee6f0b88bc47f0f570ab46fe796b2da9ccd4948971f3

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.redhat.com/en/documentation/openshift_container_platform/4.13/html-single/updating_clusters/index#updating-cluster-within-minor.

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 - 2258725 - CVE-2024-21626 runc: file descriptor leak
- BZ - 2317458 - CVE-2024-9675 buildah: Buildah allows arbitrary directory mount
- 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 - 2329817 - CVE-2024-53104 kernel: media: uvcvideo: Skip parsing frames of type UVC_VS_UNDEFINED in uvc_parse_format
- BZ - 2330539 - CVE-2024-12085 rsync: Info Leak via Uninitialized Stack Contents
- BZ - 2333122 - CVE-2024-45338 golang.org/x/net/html: Non-linear parsing of case-insensitive content in golang.org/x/net/html
- BZ - 2334412 - CVE-2024-53197 kernel: ALSA: usb-audio: Fix potential out-of-bound accesses for Extigy and Mbox devices

- BZ - 2346416 - CVE-2024-56171 libxml2: Use-After-Free in libxml2
- OCPBUGS-48085 - [4.13] Update must-gather owners (artificial PR for backports)
- OCPBUGS-50850 - [release-4.13] Increase waitForFallbackDegradedConditionTimeout of test e2e-sno-disruptive

CVEs

- CVE-2020-11023
- CVE-2022-49043
- CVE-2024-9675
- CVE-2024-11187
- CVE-2024-11218
- CVE-2024-12085
- CVE-2024-12087
- CVE-2024-12088
- CVE-2024-12747
- CVE-2024-21626
- CVE-2024-45338
- CVE-2024-50302
- CVE-2024-53104
- CVE-2024-53197
- CVE-2024-56171
- CVE-2025-1244
- CVE-2025-24928

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/.

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

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie preferences