Red Hat F

RHSA

Advis

-03-05

Overview

Synop

Importa

Type/

Security

Topic

Red Hat
updates

This rele
Platform

Red Hat
of Low. A

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

https://access.redhat.com/errata/RHBA-2026:3414

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):

None

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 x86_64 architecture. The image digest 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:a7c362225f22ef51feca9c9959409ffc5f8308a9ecc06ed2cc39b31668327eba

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 - 2376219 - CVE-2025-5987 libssh: Invalid return code for chacha20 poly1305 with OpenSSL backend
- BZ - 2396054 - CVE-2025-9230 openssl: Out-of-bounds read & write in RFC 3211 KEK Unwrap
- BZ - 2408762 - CVE-2025-6176 Scrapy: python-scrapy: brotli: Python brotli decompression bomb DoS
- BZ - 2416741 - CVE-2025-13601 glib: Integer overflow in in g_escape_uri_string()
- BZ - 2418711 - CVE-2025-66293 libpng: LIBPNG out-of-bounds read in png_image_read_composite
- BZ - 2430376 - CVE-2025-15467 openssl: OpenSSL: Remote code execution or Denial of Service via oversized Initialization Vector in CMS parsing

CVEs

- CVE-2025-5987
- CVE-2025-6176
- CVE-2025-9230
- CVE-2025-13601
- CVE-2025-15467

- CVE-2025-66293

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/.

Cool Stuff Store

Red Hat Summit
