

[Subscriptions](#) | [Downloads](#) | [Red Hat Catalog](#) | [Get Support](#)



Cookie Preferences and Opt-Out Rights

Your Choices About Cookies on this Site

i-03-05

Red Hat F

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

RHSA**Advis**

Overview

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

Synop

Importan

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Type/

Security

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Topic

Red Hat updates

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

This rele Platform


Red Hat of Low. /

Clearing your browser cookies may delete your cookie preferences. If you receives 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/>.



Quick Links 

Help 

Site Info 

Related Sites 

Loading



[About Red Hat](#)

[Jobs](#)

[Events](#)

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie Preferences and Opt-Out Rights](#)