



Red Hat Product Errata    RHSA-2024:4484 - Security Advisory

# RHSA-2024:4484 - Security Advisory

Issued: 2024-07-17    Updated: 2024-07-17

[Overview](#)[Updated Images](#)

## Synopsis

Important: OpenShift Container Platform 4.13.45 bug fix and security update

## Type/Severity

Security Advisory: Important

## Topic

Red Hat OpenShift Container Platform release 4.13.45 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 4.13.45. See the following advisory for the RPM packages for this release:

<https://access.redhat.com/errata/RHSA-2024:4486> 

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/4.13/release\\_notes/ocp-4-13-release-notes.html](https://docs.openshift.com/container-platform/4.13/release_notes/ocp-4-13-release-notes.html) 

Security Fix(es):

- golang: net/http, x/net/http2: unlimited number of CONTINUATION frames

causes DoS (CVE-2023-45288)

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

(CVE-2024-5037)

- openssh: Possible remote code execution due to a race condition in signal


handling (CVE-2024-6387)

- ssh: Prefix truncation attack on Binary Packet Protocol (BPP)

(CVE-2023-48795)


- jose-go: improper handling of highly compressed data (CVE-2024-28180)


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.openshift.com/container-platform/4.13/updating/updating-cluster-cli.html> 

## 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.openshift.com/container-platform/4.13/release\\_notes/ocp-4-13-release-notes.html](https://docs.openshift.com/container-platform/4.13/release_notes/ocp-4-13-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:c7e3658ca8f0f1fc8ce1512ecc36785a68b1388dfbfc39642bff8120bfa86a33

(For s390x architecture)

The image digest is

sha256:71641ec665a81c7228ac2254ae30899ee68bef872653c807dc34dede0cfe91b8

(For ppc64le architecture)


The image digest is

sha256:a71a1339e4304715cb0957a5db2777fd6e626420ba252af8b47445bcbfaac655

(For aarch64 architecture)

The image digest is






sha256:4f08ad2deadb6731ebd82ae924c47d06c0c162bb57914e1f287f9c0c68e9838a

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.openshift.com/container-platform/4.13/updating/updating-cluster-cli.html> 

## 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 - 2254210](#)  - CVE-2023-48795 ssh: Prefix truncation attack on Binary Packet Protocol (BPP)
- [BZ - 2268273](#)  - CVE-2023-45288 golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS
- [BZ - 2268854](#)  - CVE-2024-28180 jose-go: improper handling of highly compressed data
- [BZ - 2272339](#)  - CVE-2024-5037 openshift/telemeter: iss check during JWT authentication can be bypassed
- [BZ - 2294604](#)  - CVE-2024-6387 openssh: regreSSHion - race condition in SSH allows RCE/DoS

- [OCPBUGS-32015](#) - [release-4.13] OCPBUGS-32015: Fix zone tag value reconciliation for vSphere machines
- [OCPBUGS-34422](#) - OCP4.16 - Port\_Security flag doesn't work in ShiftonStack Srioiv Worker node deployment
- [OCPBUGS-35077](#) - [4.13] Errors not returned from wait-for-ceo cmd during bootstrap teardown
- [OCPBUGS-35380](#) - Azure CPMS periodics are failing due to non-retryable API errors
- [OCPBUGS-35857](#) - oc newapp unit tests are failing due to removed images
- [OCPBUGS-35976](#) - GHSA-6wvf-f2vw-3425: ose-installer-container: containers/image allows unexpected authenticated registry accesses
- [OCPBUGS-35990](#) - After upgrading to 4.13 from 4.12 one of the worker node went into emergency mode.
- [OCPBUGS-36501](#) - prometheus bound service token causing issues with version skew between mgmt and cluster-under-test
- [OCPBUGS-36551](#) - [Backport-4.13] TestAllowedSourceRangesStatus expected the annotation to be reflected in status.allowedSourceRanges flake

## CVEs

- [CVE-2020-12762](#)
- [CVE-2020-15778](#)
- [CVE-2020-22219](#)
- [CVE-2020-26555](#)
- [CVE-2020-28241](#)
- [CVE-2021-3782](#)
- [CVE-2021-46848](#)
- [CVE-2021-46909](#)
- [CVE-2021-46972](#)
- [CVE-2021-47069](#)
- [CVE-2021-47073](#)
- [CVE-2021-47236](#)
- [CVE-2021-47310](#)
- [CVE-2021-47311](#)
- [CVE-2021-47353](#)
- [CVE-2021-47356](#)
- [CVE-2021-47456](#)
- [CVE-2021-47495](#)
- [CVE-2021-47548](#)
- [CVE-2021-47596](#)
- [CVE-2022-4645](#)
- [CVE-2022-25308](#)
- [CVE-2022-25309](#)

- [CVE-2022-25310](#)
- [CVE-2022-27404](#)
- [CVE-2022-27405](#)
- [CVE-2022-27406](#)
- [CVE-2022-33065](#)
- [CVE-2022-36227](#)
- [CVE-2022-40023](#)
- [CVE-2022-41862](#)
- [CVE-2022-47629](#)
- [CVE-2022-48337](#)
- [CVE-2022-48339](#)
- [CVE-2022-48622](#)
- [CVE-2022-48624](#)
- [CVE-2022-48627](#)
- [CVE-2023-0666](#)
- [CVE-2023-2856](#)
- [CVE-2023-2858](#)
- [CVE-2023-2952](#)
- [CVE-2023-2953](#)
- [CVE-2023-3446](#)
- [CVE-2023-3817](#)
- [CVE-2023-4016](#)
- [CVE-2023-4408](#)
- [CVE-2023-5090](#)
- [CVE-2023-5678](#)
- [CVE-2023-6004](#)
- [CVE-2023-6597](#)
- [CVE-2023-6918](#)
- [CVE-2023-7104](#)
- [CVE-2023-25193](#)
- [CVE-2023-28450](#)
- [CVE-2023-31486](#)
- [CVE-2023-32681](#)
- [CVE-2023-37328](#)
- [CVE-2023-40474](#)
- [CVE-2023-40475](#)
- [CVE-2023-40476](#)
- [CVE-2023-43785](#)
- [CVE-2023-43786](#)
- [CVE-2023-43787](#)

- [CVE-2023-43788](#)
- [CVE-2023-43789](#)
- [CVE-2023-45229](#)
- [CVE-2023-45231](#)
- [CVE-2023-45235](#)
- [CVE-2023-45236](#)
- [CVE-2023-45237](#)
- [CVE-2023-45287](#)
- [CVE-2023-45288](#)
- [CVE-2023-45289](#)
- [CVE-2023-45290](#)
- [CVE-2023-46316](#)
- [CVE-2023-48795](#)
- [CVE-2023-50387](#)
- [CVE-2023-50868](#)
- [CVE-2023-51714](#)
- [CVE-2023-52425](#)
- [CVE-2023-52464](#)
- [CVE-2023-52560](#)
- [CVE-2023-52615](#)
- [CVE-2023-52626](#)
- [CVE-2023-52638](#)
- [CVE-2023-52667](#)
- [CVE-2023-52669](#)
- [CVE-2023-52675](#)
- [CVE-2023-52686](#)
- [CVE-2023-52700](#)
- [CVE-2023-52703](#)
- [CVE-2023-52781](#)
- [CVE-2023-52813](#)
- [CVE-2023-52835](#)
- [CVE-2023-52877](#)
- [CVE-2023-52878](#)
- [CVE-2023-52881](#)
- [CVE-2024-0450](#)
- [CVE-2024-1488](#)
- [CVE-2024-2398](#)
- [CVE-2024-3651](#)
- [CVE-2024-3652](#)
- [CVE-2024-4418](#)

- [CVE-2024-4467](#)
- [CVE-2024-5037](#)
- [CVE-2024-6387](#)
- [CVE-2024-24783](#)
- [CVE-2024-25062](#)
- [CVE-2024-25580](#)
- [CVE-2024-25629](#)
- [CVE-2024-26583](#)
- [CVE-2024-26584](#)
- [CVE-2024-26585](#)
- [CVE-2024-26656](#)
- [CVE-2024-26675](#)
- [CVE-2024-26720](#)
- [CVE-2024-26735](#)
- [CVE-2024-26759](#)
- [CVE-2024-26783](#)
- [CVE-2024-26801](#)
- [CVE-2024-26804](#)
- [CVE-2024-26826](#)
- [CVE-2024-26852](#)
- [CVE-2024-26859](#)
- [CVE-2024-26906](#)
- [CVE-2024-26907](#)
- [CVE-2024-26974](#)
- [CVE-2024-26982](#)
- [CVE-2024-27397](#)
- [CVE-2024-27410](#)
- [CVE-2024-28180](#)
- [CVE-2024-28182](#)
- [CVE-2024-28757](#)
- [CVE-2024-28834](#)
- [CVE-2024-32002](#)
- [CVE-2024-32004](#)
- [CVE-2024-32020](#)
- [CVE-2024-32021](#)
- [CVE-2024-32465](#)
- [CVE-2024-32487](#)
- [CVE-2024-33599](#)
- [CVE-2024-33600](#)
- [CVE-2024-33601](#)

- [CVE-2024-33602](#)
- [CVE-2024-34064](#)
- [CVE-2024-35235](#)
- [CVE-2024-35789](#)
- [CVE-2024-35835](#)
- [CVE-2024-35838](#)
- [CVE-2024-35845](#)
- [CVE-2024-35852](#)
- [CVE-2024-35853](#)
- [CVE-2024-35854](#)
- [CVE-2024-35855](#)
- [CVE-2024-35857](#)
- [CVE-2024-35888](#)
- [CVE-2024-35890](#)
- [CVE-2024-35898](#)
- [CVE-2024-35958](#)
- [CVE-2024-35959](#)
- [CVE-2024-35960](#)
- [CVE-2024-35969](#)
- [CVE-2024-36004](#)
- [CVE-2024-36005](#)
- [CVE-2024-36007](#)
- [CVE-2024-36016](#)
- [CVE-2024-36886](#)

## References

- <https://access.redhat.com/security/updates/classification/#important>

---

The Red Hat security contact is [secalert@redhat.com](mailto: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](#)