

[Red Hat Product Errata](#)    [RHSA-2024:1887 - Security Advisory](#)

# RHSA-2024:1887 - Security Advisory

Issued: 2024-04-25    Updated: 2024-04-25

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

## Synopsis

Important: OpenShift Container Platform 4.15.10 bug fix and security update

## Type/Severity

Security Advisory: Important

## Topic

Red Hat OpenShift Container Platform release 4.15.10 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 4.15.

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

<https://access.redhat.com/errata/RHSA-2024:1892> 

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/4.15/release\\_notes/ocp-4-15-release-notes.html](https://docs.openshift.com/container-platform/4.15/release_notes/ocp-4-15-release-notes.html) 

Security Fix(es):


- go-git: Maliciously crafted Git server replies can cause DoS on go-git

clients (CVE-2023-49568)

- cluster-monitoring-operator: credentials leak (CVE-2024-1139)
- opentelemetry-go-contrib: DoS vulnerability in otelgrpc due to unbound


cardinality metrics (CVE-2023-47108)


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 4.15 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/4.15/updating/updating\\_a\\_cluster/updating-cluster-cli.html](https://docs.openshift.com/container-platform/4.15/updating/updating_a_cluster/updating-cluster-cli.html) 

## Solution

For OpenShift Container Platform 4.15 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/4.15/release\\_notes/ocp-4-15-release-notes.html](https://docs.openshift.com/container-platform/4.15/release_notes/ocp-4-15-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

sha256:7111fb4cec202cb758f58d9bed95a67e7fdc417353ef15be56d7bf96356909d4

(For s390x architecture)

The image digest is

sha256:3dd4771c36e66984070fce29d4498d4047f4d54aaf2763758f5fb077c7e1348c

(For ppc64le architecture)


The image digest is

sha256:87856c84d81c70fb57151720cff19f90ef7c44c9c36005c8c7e8739f772dc4be

(For aarch64 architecture)

The image digest is









sha256:ef5e1f9b9cbe3ac42323a6aab66ee436fe12adf1c0623d17213d0fbfe45c2ba8

All OpenShift Container Platform 4.15 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/4.15/updating/updating\\_a\\_cluster/updating-cluster-cli.html](https://docs.openshift.com/container-platform/4.15/updating/updating_a_cluster/updating-cluster-cli.html) 

## Affected Products

- Red Hat OpenShift Container Platform 4.15 for RHEL 9 x86\_64
- Red Hat OpenShift Container Platform 4.15 for RHEL 8 x86\_64
- Red Hat OpenShift Container Platform for Power 4.15 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.15 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.15 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.15 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.15 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.15 for RHEL 8 aarch64

## Fixes

- BZ - 2251198  - CVE-2023-47108 opentelemetry-go-contrib: DoS vulnerability in otelgrpc due to unbound cardinality metrics
- BZ - 2258165  - CVE-2023-49568 go-git: Maliciously crafted Git server replies can cause DoS on go-git clients
- BZ - 2262158  - CVE-2024-1139 cluster-monitoring-operator: credentials leak
- OCPBUGS-25985  - when baselinecapability set is set to None, still see SA with name `deployer-controller` being present in the cluster
- OCPBUGS-27029  - nodeip-configuration doesn't log to serial console
- OCPBUGS-28769  - CVE-2024-1139 cluster-monitoring-operator-container: cluster-monitoring-operator: credentials leak [openshift-4.15]
- OCPBUGS-29922  - [4.15] Infinite PODs loop creation with "NodeAffinity" status
- OCPBUGS-30138  - PTP service annotated with certificate error

- [OCPBUGS-30306](#) - tuned: tuned breaks dynamic IRQ affinity
- [OCPBUGS-30507](#) - On SNO with DU profile(RT kernel) tuned profile is always degraded due to net.core.busy\_read, net.core.busy\_poll and kernel.numa\_balancing sysctl not existing in RT kernel
- [OCPBUGS-31081](#) - ovnkube-node doesn't refresh certificates after node was suspended for 30 days
- [OCPBUGS-31335](#) - Compute server group policy is not honoured
- [OCPBUGS-31348](#) - With workload partitioning enabled, setting cpu\_manager to static and having reserved cpu causes kubelet fail to restart
- [OCPBUGS-31469](#) - 4.15 Do imports on imagestreams respect ImageTagMirrorSet?
- [OCPBUGS-31471](#) - HyperShift: Minimize container ephemeral storage usage when auditing is enabled
- [OCPBUGS-31500](#) - [release-4.15] Egress IP multi NIC: ipv6 does not work
- [OCPBUGS-31503](#) - Bump to kubernetes 1.28.8
- [OCPBUGS-31538](#) - dualStack HostPrefix validation failures for non-(sdn/ovn) plugins
- [OCPBUGS-31599](#) - [csi-snapshot-controller-operator] does not create suitable role and roleBinding for csi-snapshot-webhook
- [OCPBUGS-31619](#) - Installation fails with 1 master and 2 workers as the console deployment set the number of replicas based on the InfrastructureTopology rather than the ControlPlaneTopology
- [OCPBUGS-31651](#) - [release-4.15]: Default catalog source pod never get updates
- [OCPBUGS-31667](#) - PTP consumer deployed with sidecar cannot get PTP events on getCurrentState call
- [OCPBUGS-31670](#) - Forklift operator fails on OpenShift 4.15
- [OCPBUGS-31754](#) - Invalid memory address or nil pointer dereference in Cloud Network Config Controller
- [OCPBUGS-31764](#) - gstreamer1 package dependency in network-tools creates legal concerns
- [OCPBUGS-31807](#) - api-int Certificate Authority rotation during 4.14.17 to 4.15.3 update

## CVEs

- [CVE-2023-4408](#)
- [CVE-2023-5517](#)
- [CVE-2023-5679](#)
- [CVE-2023-6240](#)
- [CVE-2023-6516](#)
- [CVE-2023-45288](#)
- [CVE-2023-47108](#)
- [CVE-2023-49568](#)
- [CVE-2023-50387](#)
- [CVE-2023-50868](#)

- [CVE-2024-1139](#) ↗
- [CVE-2024-1488](#) ↗
- [CVE-2024-26582](#) ↗
- [CVE-2024-26584](#) ↗
- [CVE-2024-26586](#) ↗

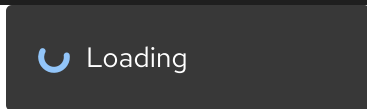
## References

- <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/>.



The image shows a dark-themed navigation menu for Red Hat. At the top left is the Red Hat logo (a red hat icon) and the text "Red Hat". To the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below these are four menu items, each with a downward-pointing chevron icon on the right: "Quick Links", "Help", "Site Info", and "Related Sites".



A dark grey rectangular button with a blue circular loading spinner icon and the text "Loading".



The footer area features a dark background with a light grey hat icon on the left. To its right, the text "About Red Hat" is displayed, followed by two lines of smaller text: "Jobs" and "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](#)