# RHSA-2024:1891 - Security Advisory

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



## Synopsis

Important: OpenShift Container Platform 4.14.22 bug fix and security update

## Type/Severity

Security Advisory: Important

## Topic

Red Hat OpenShift Container Platform release 4.14.22 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 4.14.

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

https://access.redhat.com/errata/RHSA-2024:1897

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/4.14/release_notes/ocp-4-14-release-notes.html

Security Fix(es):

- go-git: Maliciously crafted Git server replies can lead to path traversal

and RCE on go-git clients (CVE-2023-49569)

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

clients (CVE-2023-49568)

- kubevirt-csi: PersistentVolume allows access to HCP's root node

(CVE-2024-1725)

- golang.org/x/net/html: Cross site scripting (CVE-2023-3978)
- 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 4.14 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/4.14/updating/updating_a_cluster/updating-cluster-cli.html

## Solution

For OpenShift Container Platform 4.14 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/4.14/release_notes/ocp-4-14-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
sha256:7093fa606debe63820671cc92a1384e14d0b70058d4b4719d666571e1fc62190

(For s390x architecture)
The image digest is
sha256:784621b67af470153f02521237b8170fed3d58d31333b4b094cf30f6d657e40e

(For ppc64le architecture)
The image digest is
sha256:6cedfcf05100b51d7dab8ac4c0ea8c06aac8989143a3d564daf5b8041120e3ae

(For aarch64 architecture)
The image digest is
sha256:7c13402788d2e98964fa6e53b435b02b62d71769ce6c66fb4cf7d0116c7a33c6

All OpenShift Container Platform 4.14 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/4.14/updating/updating_a_cluster/updating-cluster-cli.html

## Affected Products

- Red Hat OpenShift Container Platform 4.14 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.14 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.14 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.14 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 8 aarch64

## Fixes

- BZ - 2228689 - CVE-2023-3978 golang.org/x/net/html: Cross site scripting
- BZ - 2251198 - CVE-2023-47108 opentelemetry-go-contrib: DoS vulnerability in otelgrpc due to unbound cardinality metrics
- BZ - 2258143 - CVE-2023-49569 go-git: Maliciously crafted Git server replies can lead to path traversal and RCE on go-git clients
- BZ - 2258165 - CVE-2023-49568 go-git: Maliciously crafted Git server replies can cause DoS on go-git clients
- BZ - 2265398 - CVE-2024-1725 kubevirt-csi: PersistentVolume allows access to HCP's root node

- OCPBUGS-25145 - VSphereConnectionForm link uncorrect resources
- OCPBUGS-30898 - Azure MAO CredentialsRequest Contains Unnecessary virtualMachines/extensions Permissions
- OCPBUGS-31504 - Bump to kubernetes 1.27.12
- OCPBUGS-31669 - Cluster-network-operator doesn't use node local kube-apiserver loadbalancer when templating in cluster resources
- OCPBUGS-31677 - [release-4.14] coreos-installer iso kargs show broken on Agent ISO
- OCPBUGS-31844 - tuned: tuned breaks dynamic IRQ affinity
- OCPBUGS-31862 - gstreamer1 package dependency in network-tools creates legal concerns
- OCPBUGS-31885 - Number of configured control plane replicas should be validated
- OCPBUGS-32112 - Invalid memory address or nil pointer dereference in Cloud Network Config Controller
- OCPBUGS-32137 - PTP consumer deployed with sidecar cannot get PTP events on getCurrentState call
- OCPBUGS-27108 - MCO the content mismatch bug revised when upgrading from 4.13.23 to 4.14.3
- OCPBUGS-31487 - kdump doesn't create the dumpfile via ssh with OVN
- OCPBUGS-31648 - Connection problems with OVN-Kubernetes on OpenShift Container Platform 4.12 on AWS post hibernation
- OCPBUGS-31731 - SELinux: kubelet running with wrong label [release-4.15]
- OCPBUGS-31886 - [csi-snapshot-controller-operator] does not create suitable role and roleBinding for csi-snapshot-webhook

## CVEs

- CVE-2023-3978
- CVE-2023-47108
- CVE-2023-49568
- CVE-2023-49569
- CVE-2024-1139
- CVE-2024-1725

## 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/.

Red Hat

Quick Links

Help

Site Info

Related Sites

All systems operational

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