



Red Hat Product Errata RHSA-2024:1567 - Security Advisory

RHSA-2024:1567 - Security Advisory

Issued: 2024-04-03 Updated: 2024-04-03

[Overview](#)

[Updated Packages](#)

Synopsis

Important: OpenShift Container Platform 4.14.19 security update

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

Topic

Red Hat OpenShift Container Platform release 4.14.19 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.

Security Fix(es):

- golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA


payloads (CVE-2024-1394)

- 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.

Solution

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 

Details on how to access this content 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 - 2262921](#) - CVE-2024-1394 golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads
- [BZ - 2268854](#) - CVE-2024-28180 jose-go: improper handling of highly compressed data

CVEs

- [CVE-2024-1394](#)
- [CVE-2024-28180](#)

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/>.



The image shows the Red Hat logo (a red hat icon) and the text "Red Hat" in white on a dark background. To the right of the logo are four social media icons: LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a navigation menu with four items: "Quick Links", "Help", "Site Info", and "Related Sites". Each item has a white downward-pointing chevron icon to its right. The entire menu is enclosed in a dark grey box with horizontal lines separating the items.

✓ 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](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie preferences](#)