



Red Hat Product Errata RHSA-2024:6054 - Security Advisory

RHSA-2024:6054 - Security Advisory

Issued: 2024-08-29 Updated: 2024-08-29

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

Synopsis

Important: ACS 4.4 enhancement and security update

Type/Severity

Security Advisory: Important

Topic

Updated images are now available for Red Hat Advanced Cluster Security (RHACS). The updated image includes security and bug fixes.

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

This release of RHACS 4.4.5 includes security fixes for CVE-2024-37298, CVE-2024-3727 and CVE-2024-6104. If you are using an earlier version of RHACS 4.4, you are advised to upgrade to this patch release 4.4.5.

Security issues fixed:

- gorilla/schema: Potential memory exhaustion attack due to sparse slice deserialization (CVE-2024-37298)
- containers/image: digest type does not guarantee valid type (CVE-2024-3727)
- go-retryablehttp: [↗](#) url might write sensitive information to log file (CVE-2024-6104)

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

Solution

If you are using an earlier version of RHACS 4.4, you are advised to upgrade to this patch release 4.4.5.

Affected Products

- Red Hat Advanced Cluster Security for Kubernetes 4 x86_64
- Red Hat Advanced Cluster Security for Kubernetes for IBM Z and LinuxONE 4 s390x
- Red Hat Advanced Cluster Security for Kubernetes for IBM Power, little endian 4 ppc64le

Fixes

- BZ - 2274767 [↗](#) - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- BZ - 2294000 [↗](#) - CVE-2024-6104 go-retryablehttp: url might write sensitive information to log file
- BZ - 2295010 [↗](#) - CVE-2024-37298 gorilla/schema: Potential memory exhaustion attack due to sparse slice deserialization
- ROX-25956 [↗](#) - Release RHACS 4.4.5

CVEs


- CVE-2022-48624 [↗](#)
- CVE-2023-2953 [↗](#)
- CVE-2024-1737 [↗](#)
- CVE-2024-1975 [↗](#)
- CVE-2024-2398 [↗](#)
- CVE-2024-3651 [↗](#)
- CVE-2024-3727 [↗](#)
- CVE-2024-6104 [↗](#)
- CVE-2024-6345 [↗](#)
- CVE-2024-24806 [↗](#)
- CVE-2024-25629 [↗](#)
- CVE-2024-28182 [↗](#)
- CVE-2024-32487 [↗](#)

- [CVE-2024-37298](#)
- [CVE-2024-37370](#)
- [CVE-2024-37371](#)
- [CVE-2024-37891](#)

References

- <https://access.redhat.com/security/updates/classification/#important>
- https://docs.openshift.com/acs/4.4/release_notes/44-release-notes.html

The Red Hat security contact is secalert@redhat.com. More contact details at <https://access.redhat.com/security/team/contact/>.



The image shows a dark-themed navigation bar for the Red Hat website. On the left is the Red Hat logo, consisting of a red fedora hat icon and the text "Red Hat". On the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a vertical list of navigation items: "Quick Links", "Help", "Site Info", and "Related Sites". Each item has a downward-pointing chevron icon to its right, indicating a dropdown menu.

✓ All systems operational



The image shows a dark-themed footer navigation menu. It starts with a small, light-colored fedora hat icon. Below the icon are three text links: "About Red Hat", "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 and Opt-Out Rights](#)