



# RHSA-2025:1468 - Security Advisory

Issued: 2025-02-13    Updated: 2025-02-13

[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 for Kubernetes (RHACS). The updated image includes security 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 4.4.8 includes security fixes. If you are using an earlier version of RHACS 4.4, you are advised to upgrade to this patch release 4.4.8.

Security issues fixed:

- `npm-serialize-javascript`: Cross-site Scripting (XSS) in `serialize-javascript` (CVE-2024-11831)
- `go-git`: Argument injection via the URL field (CVE-2025-21613)

- go-git: Go-git clients vulnerable to DoS via maliciously crafted Git server replies (CVE-2025-21614)
- golang.org/x/crypto/ssh: Misuse of ServerConfig.PublicKeyCallback may cause authorization bypass in golang.org/x/crypto (CVE-2024-45337)
- golang.org/x/net/html: Non-linear parsing of case-insensitive content in golang.org/x/net/html (CVE-2024-45338)

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

If you are using an earlier version of RHACS 4.4, you are advised to upgrade to this patch release 4.4.8.

## 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 - 2312579 [↗](#) - CVE-2024-11831 npm-serialize-javascript: Cross-site Scripting (XSS) in serialize-javascript
- BZ - 2331720 [↗](#) - CVE-2024-45337 golang.org/x/crypto/ssh: Misuse of ServerConfig.PublicKeyCallback may cause authorization bypass in golang.org/x/crypto
- BZ - 2333122 [↗](#) - CVE-2024-45338 golang.org/x/net/html: Non-linear parsing of case-insensitive content in golang.org/x/net/html
- BZ - 2335888 [↗](#) - CVE-2025-21613 go-git: argument injection via the URL field
- BZ - 2335901 [↗](#) - CVE-2025-21614 go-git: go-git clients vulnerable to DoS via maliciously crafted Git server replies
- ROX-27933 [↗](#) - Release RHACS 4.4.8

## CVEs

- CVE-2019-12900 [↗](#)
- CVE-2020-11023 [↗](#)
- CVE-2024-9287 [↗](#)
- CVE-2024-10041 [↗](#)
- CVE-2024-10963 [↗](#)
- CVE-2024-11168 [↗](#)
- CVE-2024-11831 [↗](#)

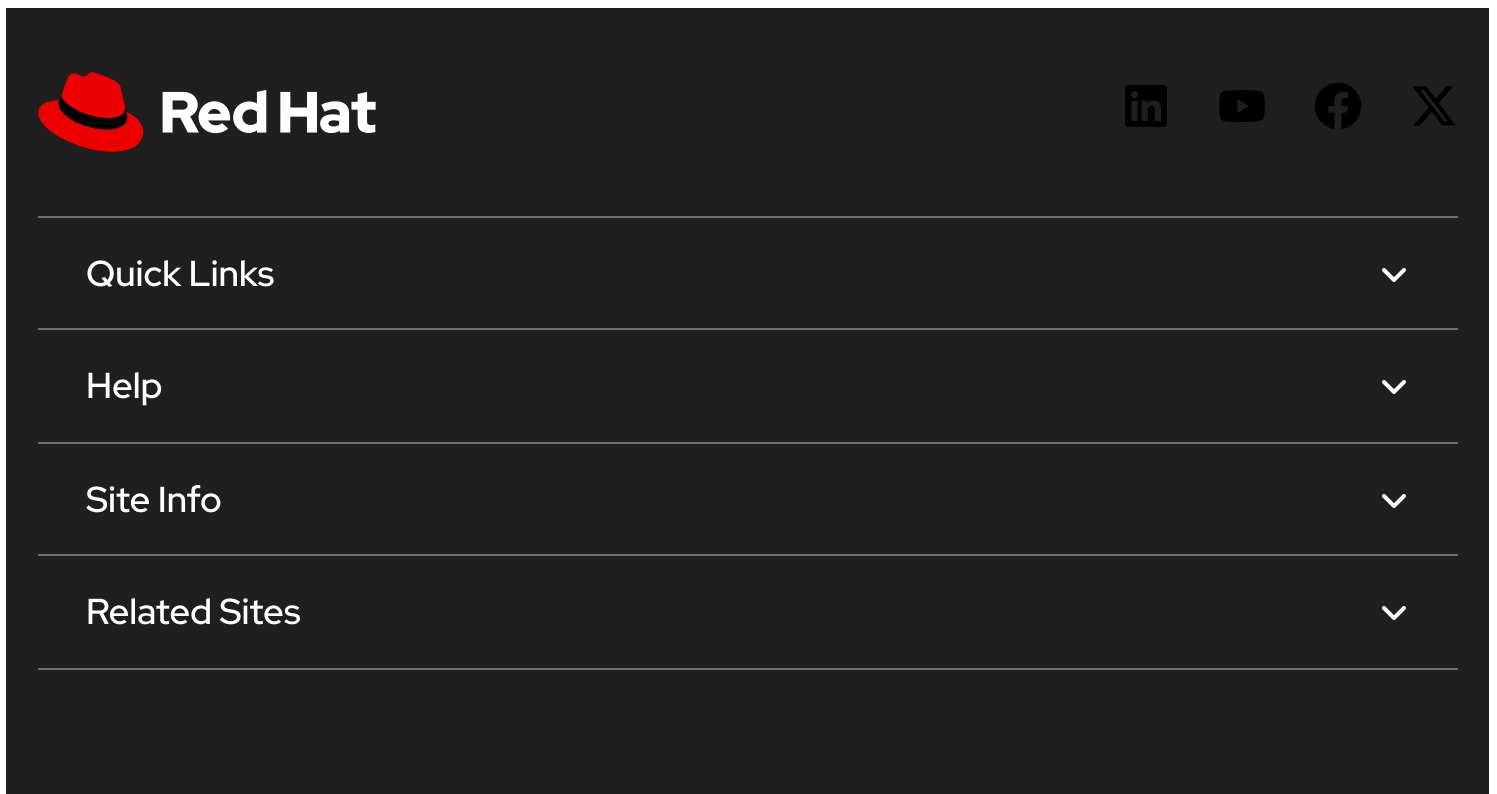
- [CVE-2024-12085](#)
- [CVE-2024-35195](#)
- [CVE-2024-45337](#)
- [CVE-2024-45338](#)
- [CVE-2025-21613](#)
- [CVE-2025-21614](#)

## References


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

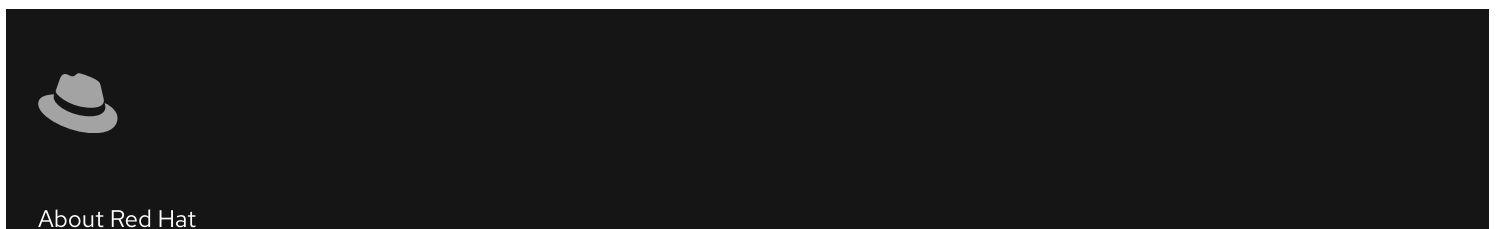
---

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 bar for the Red Hat website. On the left is the Red Hat logo, which consists of a red fedora hat icon and the text "Red Hat" in white. To the right of the logo are four social media icons: LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a vertical list of four menu items: "Quick Links", "Help", "Site Info", and "Related Sites". Each menu item is followed by a white downward-pointing chevron icon, indicating that these are expandable dropdown menus.

 All systems operational



The image shows a dark-themed footer section. On the left is a small, light-colored icon of a fedora hat. To the right of the icon is the text "About Red Hat" in a light color.

[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](#)