



RHSA-2025:1334 - Security Advisory

Issued: 2025-02-11 Updated: 2025-02-11

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

Synopsis

Important: ACS 4.5 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 fixes.

Description

This release of RHACS includes fixes for the following security vulnerabilities:

- `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`: 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)

Solution

If you are using an earlier version of RHACS 4.5, you are advised to upgrade to this patch release 4.5.6.

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-27932](#) - Release RHACS 4.5.6

CVEs

- [CVE-2024-11831](#)
- [CVE-2024-45337](#)
- [CVE-2024-45338](#)
- [CVE-2025-21613](#)
- [CVE-2025-21614](#)

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/>.



Quick Links



Help



Site Info



Related Sites



 Partial system outage



[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 and Opt-Out Rights