



# RHSA-2025:7624 - Security Advisory

Issued: 2025-05-14

Updated: 2025-05-14

[Overview](#)[Updated Packages](#)

## Synopsis

Moderate: Satellite 6 Client Bug Fix Update

## Type/Severity

Security Advisory: Moderate

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

## Topic

Updated Satellite Client packages that fix several bugs are now available for Red Hat Satellite.

Red Hat Product Security has rated this update as having a security impact of Moderate. 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 Satellite is a system management solution that allows organizations to configure and maintain their systems without the necessity to provide public Internet access to their servers or other client systems. It performs provisioning and configuration management of predefined standard operating environments.

### Security Fix(es):

- foreman\_ygg\_worker: net/http: [↗](#) sensitive headers incorrectly sent after cross-domain redirect (CVE-2024-45336)
- foreman\_ygg\_worker: Golang FIPS zeroed buffer (CVE-2024-9355)
- yggdrasil: net/http: [↗](#) sensitive headers incorrectly sent after cross-domain redirect (CVE-2024-45336)

Users of Red Hat Satellite are advised to upgrade to these updated packages, which fix these bugs.

## Solution

Before applying this update, make sure all previously released errata relevant to your system have been applied.

For details on how to apply this update, refer to:

[https://access.redhat.com/documentation/en-us/red\\_hat\\_satellite/6.16/html/updating\\_red\\_hat\\_satellite/index](https://access.redhat.com/documentation/en-us/red_hat_satellite/6.16/html/updating_red_hat_satellite/index) [↗](#)

## Affected Products

- Red Hat Enterprise Linux for x86\_64 10 x86\_64
- Red Hat Enterprise Linux for x86\_64 9 x86\_64
- Red Hat Enterprise Linux for x86\_64 8 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 10.0 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 9.6 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 9.4 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 9.2 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 9.0 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 8.8 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 8.6 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 8.4 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 8.2 x86\_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86\_64

- Red Hat Enterprise Linux Server - AUS 9.4 x86\_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86\_64
- Red Hat Enterprise Linux Server - AUS 8.6 x86\_64
- Red Hat Enterprise Linux Server - AUS 8.4 x86\_64
- Red Hat Enterprise Linux Server - AUS 8.2 x86\_64
- Red Hat Enterprise Linux for IBM z Systems 10 s390x
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.8 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.2 s390x
- Red Hat Enterprise Linux for Power, little endian 10 ppc64le
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.8 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.2 ppc64le
- Red Hat Enterprise Linux Server - TUS 8.8 x86\_64
- Red Hat Enterprise Linux Server - TUS 8.6 x86\_64
- Red Hat Enterprise Linux Server - TUS 8.4 x86\_64
- Red Hat Enterprise Linux Server - TUS 8.2 x86\_64
- Red Hat Enterprise Linux for ARM 64 10 aarch64
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.8 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64

- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.2 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 6 for RHEL 10.0 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 6 for RHEL 9.8 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 6 for RHEL 9.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 6 for RHEL 10.0 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 6 for RHEL 9.6 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.4 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.2 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.0 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 8.8 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 8.6 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 8.4 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 8.2 x86\_64

## Fixes

- [BZ - 2315719](#) - CVE-2024-9355 golang-fips: Golang FIPS zeroed buffer

- [BZ - 2341751](#) - CVE-2024-45336 golang: net/http: net/http: sensitive headers incorrectly sent after cross-domain redirect

## CVEs


- [CVE-2024-9355](#)
- [CVE-2024-45336](#)

## References

- <https://access.redhat.com/security/updates/classification/#moderate>
- [https://access.redhat.com/documentation/en-us/red\\_hat\\_satellite/6.17/html/updating\\_red\\_hat\\_satellite/index](https://access.redhat.com/documentation/en-us/red_hat_satellite/6.17/html/updating_red_hat_satellite/index)

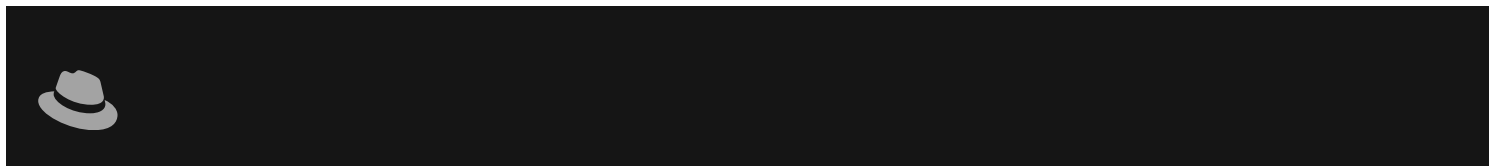
---

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 (a red hat) and the text "Red Hat". On the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below the logo are four menu items: "Quick Links", "Help", "Site Info", and "Related Sites", each with a downward-pointing chevron icon to its right.

✓ 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 and Do Not Sell or Share My Personal Information](#)