



[Red Hat Product Errata](#) [RHSA-2026:0427 - Security Advisory](#)

RHSA-2026:0427 - Security Advisory

Issued: 2026-01-12

Updated: 2026-01-12

[Overview](#)

[Updated Packages](#)

Synopsis

Moderate: libssh security update

Type/Severity

Security Advisory: Moderate

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

Topic

An update for libssh is now available for Red Hat Enterprise Linux 10.0 Extended Update Support.

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

libssh is a library which implements the SSH protocol. It can be used to implement client and server applications.

Security Fix(es):

- libssh: Invalid return code for chacha20 poly1305 with OpenSSL backend (CVE-2025-5987)

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


For details on how to apply this update, which includes the changes described in this advisory, refer to:

<https://access.redhat.com/articles/11258> 


Affected Products

- Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x
- Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le
- Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64

Fixes

- BZ - 2376219  - CVE-2025-5987 libssh: Invalid return code for chacha20 poly1305 with OpenSSL backend

CVEs

- CVE-2025-5987 

References

- <https://access.redhat.com/security/updates/classification/#moderate> 

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



✓ 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 Opt-Out Rights