



[Red Hat Product Errata](#) [RHSA-2025:17415 - Security Advisory](#)

RHSA-2025:17415 - Security Advisory

Issued: 2025-10-07 Updated: 2025-10-07

[Overview](#)

[Updated Packages](#)

Synopsis

Moderate: gnutls security, bug fix, and enhancement 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 gnutls is now available for Red Hat Enterprise Linux 8.

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

The gnutls packages provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptographic algorithms and protocols such as SSL, TLS, and DTLS.

Security Fix(es):

- gnutls: Vulnerability in GnuTLS certtool template parsing (CVE-2025-32990)
- gnutls: Vulnerability in GnuTLS otherName SAN export (CVE-2025-32988)
- gnutls: NULL pointer dereference in _gnutls_figure_common_ciphersuite() (CVE-2025-6395)

Bug Fix(es) and Enhancement(s):

- gnutls: Vulnerability in GnuTLS certtool template parsing (BZ#2359620)
- gnutls: Vulnerability in GnuTLS otherName SAN export (BZ#2359622)
- gnutls: NULL pointer dereference in _gnutls_figure_common_ciphersuite() (BZ#2376755)

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 8 x86_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x

Fixes

- [BZ - 2359620](#)  - CVE-2025-32990 gnutls: Vulnerability in GnuTLS certtool template parsing
- [BZ - 2359622](#)  - CVE-2025-32988 gnutls: Vulnerability in GnuTLS otherName SAN export
- [BZ - 2376755](#)  - CVE-2025-6395 gnutls: NULL pointer dereference in _gnutls_figure_common_ciphersuite()

CVEs

- [CVE-2025-6395](#)
- [CVE-2025-32988](#)
- [CVE-2025-32990](#)


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/>.



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 menu items: "Quick Links", "Help", "Site Info", and "Related Sites". Each item has a white downward-pointing chevron icon to its right, indicating a dropdown menu.

 Service under maintenance



The image shows a dark-themed footer area. On the left is a small, light-colored fedora hat icon. To its right are two lines of text: "About Red Hat" and "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](#)