



RHSA-2025:16115 - Security Advisory

Issued: 2025-09-17 Updated: 2025-09-17

[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 10.

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 SCT extension parsing (CVE-2025-32989)
- 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 SCT extension parsing (BZ#2359621)
- 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 10 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat Enterprise Linux for IBM z Systems 10 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat Enterprise Linux for Power, little endian 10 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat Enterprise Linux for ARM 64 10 aarch64
- 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 - 2359620](#) - CVE-2025-32990 gnutls: Vulnerability in GnuTLS certtool template parsing
- [BZ - 2359621](#) - CVE-2025-32989 gnutls: Vulnerability in GnuTLS SCT extension 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-2025-32989](#)
- [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/>.




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](#)