RHSA-2026:3477 - Security Advisory

Issued: 2026-03-02 Updated: 2026-03-02

Synopsis

Moderate: gnutls 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 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: Stack-based Buffer Overflow in gnutls_pkcs11_token_init() Function (CVE-2025-9820)
- gnutls: GnuTLS: Denial of Service via excessive resource consumption during certificate verification (CVE-2025-14831)

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 IBM z Systems 10 s390x
- Red Hat Enterprise Linux for Power, little endian 10 ppc64le
- Red Hat Enterprise Linux for ARM 64 10 aarch64

Fixes

- BZ - 2392528 - CVE-2025-9820 gnutls: Stack-based Buffer Overflow in gnutls_pkcs11_token_init() Function
- BZ - 2423177 - CVE-2025-14831 gnutls: GnuTLS: Denial of Service via excessive resource consumption during certificate verification

CVEs

- CVE-2025-9820
- CVE-2025-14831

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/.