



Red Hat F

# RHSA



5-03-10

Overview

Updated P

## Synop

Moderat

## 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 9.

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 9 x86\_64
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for ARM 64 9 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](mailto: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 Do Not Sell or Share My Personal Information](#)