



红帽产品

# RHSA



5-09-17

概述

更新的软件

## 概述

Moderat

## 类型/严重性

Security Advisory: Moderate

### Red Hat Lightspeed patch analysis

识别并修复受此公告影响的系统。

[查看受影响的系统](#)

## 标题

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.

## 描述

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.

## 解决方案

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

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

## 受影响的产品

- Red Hat Enterprise Linux for x86\_64 9 x86\_64
- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 9.6 x86\_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86\_64
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.6 x86\_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64

- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
- Red Hat Enterprise Linux for x86\_64 - Extended Life Cycle 9.6 x86\_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.6 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.6 s390x

## 修复

- [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()`

## CVE

- [CVE-2025-6395](#)
- [CVE-2025-32988](#)
- [CVE-2025-32989](#)
- [CVE-2025-32990](#)

## 参考

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

---

Red Hat 安全团队联络方式为 [secalert@redhat.com](mailto:secalert@redhat.com)。更多联络细节请参考 <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 Do Not Sell or Share My Personal Information](#)