



红帽产品基

# RHSA



25-05-13

概述

更新的软件

## 概述

Moderate

## 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 git-lfs 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

Git Large File Storage (LFS) replaces large files such as audio samples, videos, datasets, and graphics with text pointers inside Git, while storing the file contents on a remote server.

## Security Fix(es):

- golang: crypto/tls: panic when processing post-handshake message on QUIC connections (CVE-2023-39321)
- golang: crypto/tls: lack of a limit on buffered post-handshake (CVE-2023-39322)
- golang: net: malformed DNS message can cause infinite loop (CVE-2024-24788)
- golang: net/netip: Unexpected behavior from Is methods for IPv4-mapped IPv6 addresses (CVE-2024-24790)
- net/http: [↗](#) Denial of service due to improper 100-continue handling in net/http (CVE-2024-24791)
- golang-fips: Golang FIPS zeroed buffer (CVE-2024-9355)

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.

## Additional Changes:

For detailed information on changes in this release, see the Red Hat Enterprise Linux 9 Release Notes linked from 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 - 2237777 [↗](#) - CVE-2023-39321 golang: crypto/tls: panic when processing post-handshake message on QUIC connections
- BZ - 2237778 [↗](#) - CVE-2023-39322 golang: crypto/tls: lack of a limit on buffered post-handshake
- BZ - 2279814 [↗](#) - CVE-2024-24788 golang: net: malformed DNS message can cause infinite loop
- BZ - 2292787 [↗](#) - CVE-2024-24790 golang: net/netip: Unexpected behavior from Is methods for IPv4-mapped IPv6 addresses
- BZ - 2295310 [↗](#) - CVE-2024-24791 net/http: Denial of service due to improper 100-continue handling in net/http
- BZ - 2315719 [↗](#) - CVE-2024-9355 golang-fips: Golang FIPS zeroed buffer

## CVE

- CVE-2023-39321 [↗](#)
- CVE-2023-39322 [↗](#)
- CVE-2024-9355 [↗](#)
- CVE-2024-24788 [↗](#)
- CVE-2024-24790 [↗](#)
- CVE-2024-24791 [↗](#)

## 参考

- <https://access.redhat.com/security/updates/classification/#moderate> [↗](#)
- [https://docs.redhat.com/en/documentation/red\\_hat\\_enterprise\\_linux/9/html/9.6\\_release\\_notes/index](https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/9.6_release_notes/index) [↗](#)

---

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



 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](#)