



Red Hat Product Errata RHSA-2024:2562 - Security Advisory

RHSA-2024:2562 - Security Advisory

Issued: 2024-04-30 Updated: 2024-04-30

[Overview](#)[Updated Packages](#)

Synopsis

Important: golang security update

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#)

Topic

An update for golang is now available for Red Hat Enterprise Linux 9.

Red Hat Product Security has rated this update as having a security impact of Important. 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 golang packages provide the Go programming language compiler.

Security Fix(es):

- golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads (CVE-2024-1394)
- golang: net/http: [memory exhaustion in Request.ParseMultipartForm](#) (CVE-2023-45290)
- golang: net/http/cookiejar: incorrect forwarding of sensitive headers and cookies on HTTP redirect (CVE-2023-45289)
- golang: crypto/x509: Verify panics on certificates with an unknown public key algorithm (CVE-2024-24783)
- golang: net/mail: comments in display names are incorrectly handled (CVE-2024-24784)
- golang: html/template: errors returned from MarshalJSON methods may break template escaping (CVE-2024-24785)
- golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS (CVE-2023-45288)

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, 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 x86_64 - Extended Update Support 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 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 IBM z Systems - Extended Update Support 9.4 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 Power, little endian - Extended Update Support 9.4 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 for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x

Fixes

- [BZ - 2262921](#) - CVE-2024-1394 golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads
- [BZ - 2268017](#) - CVE-2023-45290 golang: net/http: memory exhaustion in Request.ParseMultipartForm
- [BZ - 2268018](#) - CVE-2023-45289 golang: net/http/cookiejar: incorrect forwarding of sensitive headers and cookies on HTTP redirect
- [BZ - 2268019](#) - CVE-2024-24783 golang: crypto/x509: Verify panics on certificates with an unknown public key algorithm
- [BZ - 2268021](#) - CVE-2024-24784 golang: net/mail: comments in display names are incorrectly handled
- [BZ - 2268022](#) - CVE-2024-24785 golang: html/template: errors returned from MarshalJSON methods may break template escaping
- [BZ - 2268273](#) - CVE-2023-45288 golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS

CVEs


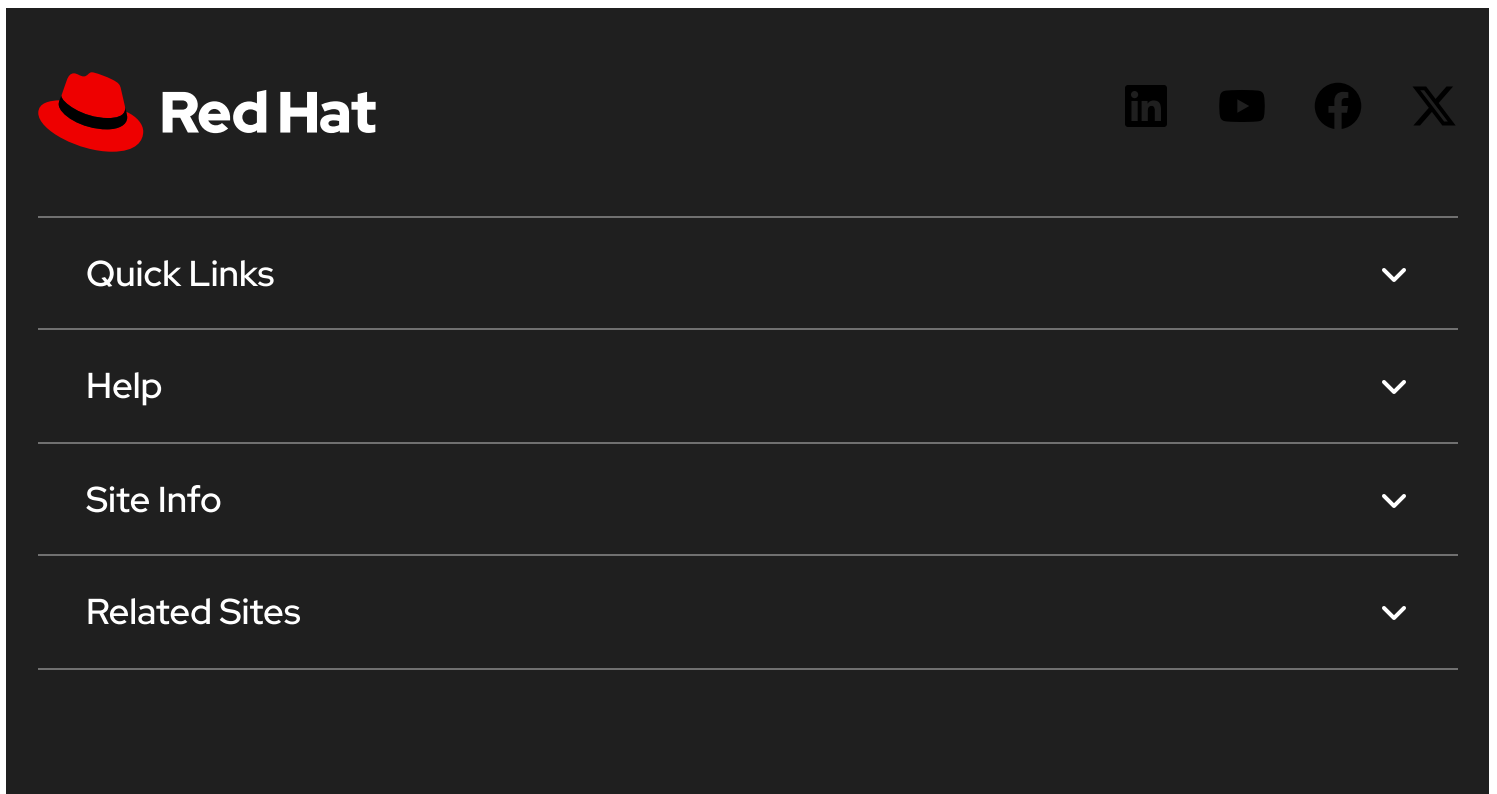
- [CVE-2023-45288](#)
- [CVE-2023-45289](#)
- [CVE-2023-45290](#)


- [CVE-2024-1394](#) 
- [CVE-2024-24783](#) 
- [CVE-2024-24784](#) 
- [CVE-2024-24785](#) 


References


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


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](#)