



Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site



Red Hat F

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

RHSA Advis

-04-30

Overview

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

Updated P

Synop

Importa

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

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 goolang 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

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 

Loading



- 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 Opt-Out Rights](#)