



Red Hat F

# RHSA Advis



4-05-23

Overview

Updated P

## Synop

Importa

## 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 etcd is now available for Red Hat OpenStack Platform 16.2 (Train).

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

A highly-available key value store for shared configuration

Security Fix(es):

- Incomplete fix for CVE-2023-39325/CVE-2023-44487 in OpenStack Platform (CVE-2024-4438)
- Incomplete fix for CVE-2021-44716 in OpenStack Platform (CVE-2024-4437)
- Incomplete fix for CVE-2022-41723 in OpenStack Platform (CVE-2024-4436)
- golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS (CVE-2023-45288)
- golang: net/http/internal: Denial of Service (DoS) via Resource Consumption via HTTP requests (CVE-2023-39326)
- golang: crypto/tls: lack of a limit on buffered post-handshake (CVE-2023-39322)
- golang: crypto/tls: panic when processing post-handshake message on QUIC connections (CVE-2023-39321)
- golang: html/template: improper handling of special tags within script contexts (CVE-2023-39319)
- golang: html/template: improper handling of HTML-like comments within script contexts (CVE-2023-39318)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page 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 OpenStack for IBM Power 16.2 ppc64le
- Red Hat OpenStack 16.2 x86\_64

## Fixes

- [BZ - 2237773](#)  - CVE-2023-39319 golang: html/template: improper handling of special tags within script contexts

- [BZ - 2237776](#) - CVE-2023-39318 golang: html/template: improper handling of HTML-like comments within script contexts
- [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 - 2253330](#) - CVE-2023-39326 golang: net/http/internal: Denial of Service (DoS) via Resource Consumption via HTTP requests
- [BZ - 2268273](#) - CVE-2023-45288 golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS
- [BZ - 2279357](#) - CVE-2024-4436 etcd: Incomplete fix for CVE-2022-41723 in OpenStack Platform
- [BZ - 2279361](#) - CVE-2024-4437 etcd: Incomplete fix for CVE-2021-44716 in OpenStack Platform
- [BZ - 2279365](#) - CVE-2024-4438 etcd: Incomplete fix for CVE-2023-39325/CVE-2023-44487 in OpenStack Platform

## CVEs

- [CVE-2023-39318](#)
- [CVE-2023-39319](#)
- [CVE-2023-39321](#)
- [CVE-2023-39322](#)
- [CVE-2023-39326](#)
- [CVE-2023-45287](#)
- [CVE-2023-45288](#)
- [CVE-2024-4436](#)
- [CVE-2024-4437](#)
- [CVE-2024-4438](#)

## References

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

---

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



✔ 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 Opt-Out Rights