



Red Hat Product Errata    RHSA-2024:2729 - Security Advisory

# RHSA-2024:2729 - Security Advisory

Issued: 2024-05-22    Updated: 2024-05-22

[Overview](#)

[Updated Packages](#)

## Synopsis

Important: Red Hat OpenStack Platform 17.1 (etcd) 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 etcd is now available for Red Hat OpenStack Platform 17.1 (Wallaby).

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):

- golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads (CVE-2024-1394)
- net/http/internal: Denial of Service (DoS) via Resource Consumption via

HTTP requests (CVE-2023-39326)

- crypto/tls: Timing Side Channel attack in RSA based TLS key exchanges.

(CVE-2023-45287)

- net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS (CVE-2023-45288)
- etcd: Incomplete fix for CVE-2023-39325/CVE-2023-44487 in OpenStack Platform (CVE-2024-4438)

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 17.1 for RHEL 9 x86\_64

## Fixes

- BZ - 2253193  - CVE-2023-45287 golang: crypto/tls: Timing Side Channel attack in RSA based TLS key exchanges.
- BZ - 2253330  - CVE-2023-39326 golang: net/http/internal: Denial of Service (DoS) via Resource Consumption via HTTP requests
- BZ - 2262921  - CVE-2024-1394 golang-fips/openssl: Memory leaks in code encrypting and decrypting RSA payloads

- [BZ - 2268273](#) - CVE-2023-45288 golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS
- [BZ - 2279365](#) - CVE-2024-4438 etcd: Incomplete fix for CVE-2023-39325/CVE-2023-44487 in OpenStack Platform

## CVEs

- [CVE-2023-39326](#)
- [CVE-2023-45287](#)
- [CVE-2023-45288](#)
- [CVE-2024-1394](#)
- [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



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 Opt-Out Rights](#)