



RHSA-2025:2067 - Security Advisory

Issued: 2025-03-03 Updated: 2025-03-03

[Overview](#)

Synopsis

Important: Red Hat Build of Apache Camel 4.8 for Quarkus 3.15 update is now available (RHBQ 3.15.3.SP1)

Type/Severity

Security Advisory: Important

Topic

An update for Red Hat Build of Apache Camel 4.8 for Quarkus 3.15 update is now available (RHBQ 3.15.3.SP1).

The purpose of this text-only errata is to inform you about the enhancements that improve your developer experience and ensure the security and stability of your products.

Red Hat Product Security has rated this update as having a security impact of Important.

Description

An update for Red Hat Build of Apache Camel 4.8 for Quarkus 3.15 update is now available (RHBQ 3.15.3.SP1).

The purpose of this text-only errata is to inform you about the enhancements that improve your developer experience and ensure the security and stability of your products:

- quarkus-resteasy: Memory Leak in Quarkus RESTEasy Classic When Client Requests Timeout (CVE-2025-1634)

- [io.quarkus/quarkus-rest: Quarkus REST Endpoint Request Parameter Leakage Due to Shared Instance \(CVE-2025-1247\)](#)
- [io.netty/netty-handler: SslHandler doesn't correctly validate packets which can lead to native crash when using native SSLEngine \(CVE-2025-24970\)](#)

Solution

Before applying the update, back up your existing installation, including all applications, configuration files, databases and database settings, and so on.

The References section of this erratum contains a download link (you must log in to download the update).

Affected Products

- Red Hat Build of Apache Camel 1 x86_64

Fixes

- [BZ - 2344787](#) - CVE-2025-24970 io.netty:netty-handler: SslHandler doesn't correctly validate packets which can lead to native crash when using native SSLEngine
- [BZ - 2345172](#) - CVE-2025-1247 io.quarkus:quarkus-rest: Quarkus REST Endpoint Request Parameter Leakage Due to Shared Instance
- [BZ - 2347319](#) - CVE-2025-1634 io.quarkus:quarkus-resteasy: Memory Leak in Quarkus RESTEasy Classic When Client Requests Timeout

CVEs

- [CVE-2025-1247](#)
- [CVE-2025-1634](#)
- [CVE-2025-24970](#)

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](#)