



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

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.

5-02-27

Overview

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

Type/

Security

Accept Default	Do Not Sell or Share My Personal
--------------------------------	---

Topic

An update is now available for Red Hat build of Quarkus.

Red Hat Product Security has rated this update as having an important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability.

For more information, see the CVE links in the References section.

Description

This release of Red Hat Build of Quarkus 3.15.3.SP1 includes security updates.

For more information, see the release notes page listed in the References section.

Security Fix(es):

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

- [io.quarkus:quarkus-resteasy: Memory Leak in Quarkus RESTEasy Classic When Client Requests Timeout \(CVE-2025-1634\)](#)

Solution

Before applying this update, ensure that all previously released errata relevant to your system are applied.

For details about applying this update, refer to:

<https://access.redhat.com/articles/11258>

Affected Products

- Red Hat build of Quarkus Text-Only Advisories 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 SSL Engine
- [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



 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 Do Not Sell or Share My Personal Information](#)