RHSA-2025:3543 - Security Advisory

Issued: 2025-04-02 Updated: 2025-04-02

Overview

Synopsis

Important: Red Hat Build of Apache Camel 4.8.5 for Spring Boot security update.

Type/Severity

Security Advisory: Important

Topic

Red Hat build of Apache Camel 4.8.5 for Spring Boot release and security update is now available.

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

Red Hat build of Apache Camel 4.8.5 for Spring Boot release and security update is now available.

The purpose of this text-only errata is to inform you about the security issues fixed.

Security Fix(es):

- json-smart: Potential DoS via stack exhaustion (incomplete fix for CVE-2023-1370) (CVE-2024-57699)
- io.smallrye/smallrye-fault-tolerance-core: SmallRye Fault Tolerance (CVE-2025-2240)

- spring-security-core: CVE-2025-22228: Spring Security BCryptPasswordEncoder does not enforce maximum password length (CVE-2025-22228)
- io.netty/netty-handler: SslHandler doesn't correctly validate packets which can lead to native crash when using native SSLEngine (CVE-2025-24970)
- org.apache.camel/camel-http: bypass of header filters via specially crafted response (CVE-2025-27636)
- org.apache.camel/camel-http-base: bypass of header filters via specially crafted response (CVE-2025-27636)

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

Before applying this update, make sure all previously released errata relevant to your system have been applied.

For details on how to apply this update, refer to:

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

Affected Products

- Red Hat Integration - Camel for Spring Boot 1 x86_64

Fixes

- BZ - 2344073 - CVE-2024-57699 json-smart: Potential DoS via stack exhaustion (incomplete fix for CVE-2023-1370)
- 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 - 2350682 - CVE-2025-27636 camel-http: org.apache.camel: bypass of header filters via specially crafted response
- BZ - 2351452 - CVE-2025-2240 smallrye-fault-tolerance: SmallRye Fault Tolerance
- BZ - 2353507 - CVE-2025-22228 spring-security-core: Spring Security BCryptPasswordEncoder does not enforce maximum password length

CVEs

- CVE-2024-57699
- CVE-2025-2240
- CVE-2025-22228
- CVE-2025-24970
- CVE-2025-27636

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/.

Red Hat

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