



Red Hat Product Errata    RHSA-2025:23143 - Security Advisory

## RHSA-2025:23143 - Security Advisory

Issued: 2025-12-11    Updated: 2025-12-11

[Overview](#)

### Synopsis

Critical: Red Hat Build of Apache Camel 4.14.2 for Spring Boot release.

### Type/Severity

Security Advisory: Critical

### Topic

Red Hat build of Apache Camel 4.14.2 for Spring Boot patch 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 4.14.2 for Spring Boot patch 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):

- undertow-core: Undertow MadeYouReset HTTP/2 DDoS Vulnerability (CVE-2025-9784)
- tika-core: Apache Tika core, Apache Tika parsers, Apache Tika PDF parser module: Update to CVE-2025-54988 to expand scope of artifacts affected (CVE-2025-66516)

## 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 - 2392306  - CVE-2025-9784 undertow: Undertow MadeYouReset HTTP/2 DDoS Vulnerability
- BZ - 2418870  - CVE-2025-66516 tika-core: tika-parsers: tika-parser-pdf-module: Apache Tika core, Apache Tika parsers, Apache Tika PDF parser module: Update to CVE-2025-54988 to expand scope of artifacts affected

## CVEs

- CVE-2025-9784 
- CVE-2025-48924 
- CVE-2025-66516 

## References

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

---

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](#)