



Red Hat Product Errata    RHSA-2026:3890 - Security Advisory

# RHSA-2026:3890 - Security Advisory

Issued: 2026-03-05    Updated: 2026-03-05

[Overview](#)

## Synopsis

Important: Red Hat Build of Apache Camel 4.14.4 for Spring Boot release.

## Type/Severity

Security Advisory: Important

## Topic

Red Hat build of Apache Camel 4.14.4 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 4.14.4 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 HTTP Server Fails to Reject Malformed Host Headers Leading to Potential Cache Poisoning and SSRF (CVE-2025-12543)
- vertx-core: static handler component cache can be manipulated to deny the access to static files (CVE-2026-1002)
- mchange-commons-java: mchange-commons-java: Arbitrary code execution via JNDI dereferencing of crafted objects (CVE-2026-27727)
- com.mchange/c3p0: c3p0: Arbitrary Code Execution via deserialization of crafted objects (CVE-2026-27830)

## 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 - 2408784  - CVE-2025-12543 undertow-core: Undertow HTTP Server Fails to Reject Malformed Host Headers Leading to Potential Cache Poisoning and SSRF
- BZ - 2430180  - CVE-2026-1002 io.vertx/vertx-core: static handler component cache can be manipulated to deny the access to static files
- BZ - 2442671  - CVE-2026-27727 com.mchange/mchange-commons-java: mchange-commons-java: Arbitrary code execution via JNDI dereferencing of crafted objects
- BZ - 2442908  - CVE-2026-27830 c3p0: c3p0: Arbitrary Code Execution via deserialization of crafted objects

## CVEs

- CVE-2025-12543 
- CVE-2026-1002 
- CVE-2026-27727 
- CVE-2026-27830 

## 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](#)