RHSA

:6-03-18

Overview

Updated Pa

Synop

Importan

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

A security update is now available for Red Hat JBoss Enterprise Application Platform 7.4 for Red Hat Enterprise Linux 8. 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 JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.24 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.23, and includes bug fixes and

enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.24 Release Notes for information about the most significant bug fixes and enhancements included in this release.

Security Fix(es):

- jackson-core: jackson-core Potential StackoverflowError (CVE-2025-52999)
- undertow-core: Undertow HTTP Server Fails to Reject Malformed Host Headers Leading to Potential Cache Poisoning and SSRF [eap-7.4.z] (CVE-2025-12543)
- cxf: CXF JMS Code Execution Vulnerability [eap-7.4.z] (CVE-2025-48913)
- netty-codec-http2: Netty MadeYouReset HTTP/2 DDoS Vulnerability (CVE-2025-55163)
- org.eclipse.jgit: XXE vulnerability in Eclipse JGit [eap-7.4.z] (CVE-2025-4949)
- hibernate-core: Hibernate: Information disclosure and data deletion via second-order SQL injection [eap-7.4.z] (CVE-2026-0603)
- com.google.protobuf/protobuf-java: StackOverflow vulnerability in Protocol Buffers (CVE-2024-7254)
- undertow: OutOfMemory when parsing form data encoding with application/x-www-form-urlencoded [eap-7.4.z] (CVE-2024-3884)
- undertow-core: Undertow MadeYouReset HTTP/2 DDoS Vulnerability (CVE-2025-9784)

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 the update, make sure all previously released errata relevant to your system have been applied. Also, back up your existing installation, including all applications, configuration files, databases and database settings. For details on how to apply this update, refer to: https://access.redhat.com/articles/11258

Affected Products

- JBoss Enterprise Application Platform 7.4 ELS 7.4 for RHEL 8 x86_64

Fixes

- BZ - 2275287 - CVE-2024-3884 undertow: OutOfMemory when parsing form data encoding with application/x-www-form-urlencoded
- BZ - 2313454 - CVE-2024-7254 protobuf: StackOverflow vulnerability in Protocol Buffers
- BZ - 2367730 - CVE-2025-4949 org.eclipse.jgit: XXE vulnerability in Eclipse JGit
- BZ - 2374804 - CVE-2025-52999 com.fasterxml.jackson.core/jackson-core: jackson-core Potential StackoverflowError
- BZ - 2387221 - CVE-2025-48913 org.apache.cxf/cxf: CXF JMS Code Execution Vulnerability
- BZ - 2388252 - CVE-2025-55163 netty: netty-codec-http2: Netty MadeYouReset HTTP/2 DDoS Vulnerability
- BZ - 2392306 - CVE-2025-9784 undertow: Undertow MadeYouReset HTTP/2 DDoS Vulnerability

- BZ - 2408784 - CVE-2025-12543 undertow-core: Undertow HTTP Server Fails to Reject Malformed Host Headers Leading to Potential Cache Poisoning and SSRF
- BZ - 2427147 - CVE-2026-0603 org.hibernate/hibernate-core: Hibernate: Information disclosure and data deletion via second-order SQL injection
- JBEAP-30075 - Tracker bug for the EAP 7.4.24 release for RHEL-8

CVEs

- CVE-2024-3884
- CVE-2024-7254
- CVE-2025-4949
- CVE-2025-9784
- CVE-2025-12543
- CVE-2025-48913
- CVE-2025-52999
- CVE-2025-55163
- CVE-2026-0603

References

- https://access.redhat.com/security/updates/classification/#important
- https://docs.redhat.com/en/documentation/red_hat_jboss_enterprise_application_platform/7.4
- https://docs.redhat.com/en/documentation/red_hat_jboss_enterprise_application_platform/7.4/html-single/installation_guide/index

---

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