RHSA-2026:6011 - Security Advisory

Issued: 2026-03-30 Updated: 2026-03-30

Synopsis

Critical: Red Hat JBoss Enterprise Application Platform 7.3.17 security update

Type/Severity

Security Advisory: Critical

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

An update is now available for Red Hat JBoss Enterprise Application Platform 7.3 for Red Hat Enterprise Linux 7. 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 7.3.17 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.16, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.17 Release Notes for information about the most significant bug fixes and enhancements included in this release.

Security Fix(es):

- hibernate-core: Hibernate: Information disclosure and data deletion via second-order SQL injection (CVE-2026-0603)
- org.eclipse.jgit: XXE vulnerability in Eclipse JGit (CVE-2025-4949)
- undertow: OutOfMemory when parsing form data encoding with application/x-www-form-urlencoded (CVE-2024-3884)
- cxf: CXF JMS Code Execution Vulnerability (CVE-2025-48913)

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, ensure 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 7.3 EUS 7.3 x86_64

Fixes

- BZ - 2275287 - CVE-2024-3884 undertow: OutOfMemory when parsing form data encoding with application/x-www-form-urlencoded
- BZ - 2367730 - CVE-2025-4949 org.eclipse.jgit: XXE vulnerability in Eclipse JGit
- BZ - 2387221 - CVE-2025-48913 org.apache.cxf/cxf: CXF JMS Code Execution Vulnerability
- BZ - 2427147 - CVE-2026-0603 org.hibernate/hibernate-core: Hibernate: Information disclosure and data deletion via second-order SQL injection
- JBEAP-31431 - Tracker bug for the EAP 7.3.17 release for RHEL-7

CVEs

- CVE-2024-3884
- CVE-2025-4949
- CVE-2025-48913
- CVE-2026-0603

References

- https://access.redhat.com/security/updates/classification/#critical
- https://docs.redhat.com/en/documentation/red_hat_jboss_enterprise_application_platform/7.3
- https://docs.redhat.com/en/documentation/red_hat_jboss_enterprise_application_platform/7.3/html-single/installation_guide/index
- https://docs.redhat.com/en/documentation/red_hat_jboss_enterprise_application_platform/7.3/html/7.3.0_release_notes/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

Loading