RHSA-2026:3892 - Security Advisory

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

Overview

Synopsis

Important: Red Hat JBoss Enterprise Application Platform 8.0.12 security update

Type/Severity

Security Advisory: Important

Topic

A security update is now available for Red Hat JBoss Enterprise Application Platform 8.0. 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 8 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 8.0.12 serves as a replacement for Red Hat JBoss Enterprise Application Platform 8.0.11, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 8.0.12 Release Notes for information about the most significant bug fixes and enhancements included in this release.

Security Fix(es):

- undertow-core: Undertow HTTP Server Fails to Reject Malformed Host Headers

Leading to Potential Cache Poisoning and SSRF [eap-8.0.z] (CVE-2025-12543)

- undertow-core: Undertow MadeYouReset HTTP/2 DDoS Vulnerability (CVE-2025-9784)
- undertow: OutOfMemory when parsing form data encoding with

application/x-www-form-urlencoded [eap-8.0.z] (CVE-2024-3884)

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 Text-Only Advisories x86_64

Fixes

- BZ - 2275287 - CVE-2024-3884 undertow: OutOfMemory when parsing form data encoding with application/x-www-form-urlencoded
- 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
- JBEAP-31251 - [GSS](8.0.z) Upgrade hibernate-orm from 6.2.46 to version 6.2.49
- JBEAP-31325 - [GSS](8.0.z) Upgrade WildFly Elytron from 2.2.12.Final-redhat-00002 to 2.2.13.Final-redhat-00001

- JBEAP-31343 - [GSS](8.0.z) CXF-9171 - DelayedCachedOutputStreamCleaner thread accumulation after CVE-2025-23184 fix
- JBEAP-31397 - [GSS](8.0.z) Upgrade org.jboss.spec.jakarta.el:jboss-el-api_5_0_spec to 4.0.2.Final-redhat-00001
- JBEAP-31420 - [GSS](8.0.z) Upgrade jboss-eap-installation-manager (prospero) to 1.1.20.Final
- JBEAP-31438 - [GSS](8.0.z) Upgrade RESTEasy from 6.2.12.Final-redhat-00001 to 6.2.15.Final
- JBEAP-31446 - [GSS](8.0.z) Upgrade Apache CXF from 4.0.9.redhat-00002 to 4.0.10.redhat-00001
- JBEAP-31453 - [GSS](8.0.z) Upgrade Migration Tool for EAP 8.0 Update 12
- JBEAP-31566 - [GSS](8.0.z) Upgrade JBossWS-CXF from 7.3.6.Final-redhat-00001 to 7.3.7.Final-redhat-00001
- JBEAP-31579 - [GSS](8.0.z) Upgrade WildFly Elytron from 2.2.13.Final-redhat-00001 to 2.2.14.Final-redhat-00001
- JBEAP-31596 - (8.0.z) Upgrade yasson from 3.0.4.redhat-00004 to 3.0.4.redhat-00006
- JBEAP-31679 - (8.0.z) Upgrade WildFly Core from 21.0.18.Final-redhat-00001 to 21.0.19.Final-redhat-00001
- JBEAP-31708 - (8.0.z) Upgrade WildFly Core from 21.0.19.Final-redhat-00001 to 21.0.20.Final-redhat-00001
- JBEAP-31712 - (8.0.z) Update EAP channel to use wildfly-ee-feature-pack-product-conf x.x.x in EAP 8.0 Update 12
- JBEAP-31073 - (8.0.z) Upgrade EAP codebase in EAP 8.0 Update 12

CVEs

- CVE-2024-3884
- CVE-2025-9784
- CVE-2025-12543

References

- https://access.redhat.com/security/updates/classification/#important
- https://docs.redhat.com/en/documentation/red_hat_jboss_enterprise_application_platform/8.0
- https://docs.redhat.com/en/documentation/red_hat_jboss_enterprise_application_platform/8.0/html/release_notes_for_red_hat_jboss_enterprise_ap
- https://access.redhat.com/articles/7134189

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.