RHSA-2026:0383 - Security Advisory

Issued: 2026-01-08 Updated: 2026-01-08

Synopsis

Important: Red Hat JBoss Enterprise Application Platform 8.1.3 security update

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 8.1 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 8 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 8.1.3 serves as a replacement for Red Hat JBoss Enterprise Application Platform 8.1.2, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 8.1.3 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-8.1.z] (CVE-2025-12543)
- undertow: OutOfMemory when parsing form data encoding with application/x-www-form-urlencoded [eap-8.1.z] (CVE-2024-3884)
- undertow-core: Undertow MadeYouReset HTTP/2 DDoS Vulnerability [eap-8.1.z] (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 8.1 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 - 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-31373 - Tracker bug for the EAP 8.1.3 release for RHEL-8
- JBEAP-30596 - (8.1.z) Upgrade Undertow from 2.3.18.SP1-redhat-00001 to 2.3.20.SP2-redhat-00001
- JBEAP-31250 - [GSS](8.1.z) Upgrade hibernate ORM from 6.6.31.Final-redhat-00001 to 6.6.36.Final-redhat-00001
- JBEAP-31326 - (8.1.z) Upgrade WildFly Elytron from 2.6.5.Final-redhat-00001 to 2.6.6.Final-redhat-00001
- JBEAP-31344 - [GSS](8.1.z) CXF-9171 - DelayedCachedOutputStreamCleaner thread accumulation after CVE-2025-23184 fix
- JBEAP-31345 - (8.1.z) Upgrade WildFly Core from 27.1.2.Final-redhat-00002 to 27.1.3.Final-redhat-00001
- JBEAP-31380 - [GSS](8.1.z) Upgrade JBoss EAP to 8.1.1.GA-redhat-00007 in 8.1 Update 3
- JBEAP-31396 - [GSS](8.1.z) Upgrade org.jboss.spec.jakarta.el:jboss-el-api_5_0_spec from 4.0.1.Final-redhat-00001 to 4.0.2.Final-redhat-00001
- JBEAP-31414 - [GSS](8.1.z) Upgrade Apache CXF from 4.0.9.redhat-00002 to 4.0.10.redhat-00001
- JBEAP-31421 - [GSS](8.1.z) Upgrade wildfly-clustering from 5.0.11.Final-redhat-00001 to 5.0.12.Final-redhat-00001
- JBEAP-31474 - [GSS](8.1.z) Upgrade JBoss Threads from 2.4.0.Final-redhat-00001 to 2.5.0.redhat-00001
- JBEAP-31494 - [GSS](8.1.z) Upgrade galleon-plugins from 7.3.1.Final-redhat-00003 to 7.3.2.Final
- JBEAP-31495 - (8.1.z) Upgrade eap-maven-plugin to 2.0.1.Final
- JBEAP-31601 - (8.1.z) Upgrade Undertow from 2.3.20.SP2-redhat-00001 to 2.3.20.SP4-redhat-00001

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/8.1
- https://docs.redhat.com/en/documentation/red_hat_jboss_enterprise_application_platform/8.1/html/release_notes_for_red_hat_jboss_enterprise_ap
- https://docs.redhat.com/en/documentation/red_hat_jboss_enterprise_application_platform/8.1/html/red_hat_jboss_enterprise_application_platform_
- https://access.redhat.com/articles/7134190

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