RHSA-2025:3467 - Security Advisory

Issued: 2025-04-01 Updated: 2025-10-23

Overview

Synopsis

Important: Red Hat JBoss Enterprise Application Platform 7.4.21 security update

Type/Severity

Security Advisory: Important

Topic

A security update is now available for Red Hat JBoss Enterprise Application Platform 7.4.

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.

[Updated 5 November 2025]
The Synopsis was updated to fix a typo in the product version (7.4.21). No other changes have been made.

Description

Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime.

This asynchronous patch is a security update for Red Hat JBoss Enterprise Application Platform 7.4.

Security Fix(es):

- io.netty/netty: Denial of Service attack on windows app using Netty (CVE-2024-47535)
- netty-common: Denial of Service attack on windows app using Netty (CVE-2025-25193)
- io.netty/netty-handler: SslHandler doesn't correctly validate packets which can lead to native crash when using native SSLEngine (CVE-2025-24970)

- org.wildfly.core/wildfly-server: Wildfly improper RBAC permission (CVE-2025-23367)
- hornetq-core-client: Arbitrarily overwrite files or access sensitive information Security (CVE-2024-51127)

A Red Hat Security Bulletin which addresses further details about this flaw is available in the References section.

For more details about the security issue(s), including the impact, a CVSS score, acknowledgements, 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 - 2323697 - CVE-2024-51127 hornetq-core-client: Arbitrarily overwrite files or access sensitive information
- BZ - 2325538 - CVE-2024-47535 netty: Denial of Service attack on windows app using Netty
- BZ - 2337620 - CVE-2025-23367 org.wildfly.core:wildfly-server: Wildfly improper RBAC permission
- BZ - 2344787 - CVE-2025-24970 io.netty:netty-handler: SslHandler doesn't correctly validate packets which can lead to native crash when using native SSLEngine
- BZ - 2344788 - CVE-2025-25193 netty: Denial of Service attack on windows app using Netty

CVEs

- CVE-2024-47535
- CVE-2024-51127
- CVE-2025-23367
- CVE-2025-24970
- CVE-2025-25193
- CVE-2025-48734
- CVE-2025-52999

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/.