Red Hat P

RHSA

25-07-14

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 9. 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 7.4.23 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.22, and includes bug fixes and

enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.23 Release Notes for information about the most significant bug fixes and enhancements included in this release.

Security Fix(es):

- commons-beanutils-core: Apache Commons BeanUtils: PropertyUtilsBean does not suppresses an enum's declaredClass property by default [eap-7.4.z] (CVE-2025-48734)
- commons-beanutils: Apache Commons BeanUtils: PropertyUtilsBean does not suppresses an enum's declaredClass property by default [eap-7.4.z] (CVE-2025-48734)
- commons-beanutils-commons-beanutils: Apache Commons BeanUtils: PropertyUtilsBean does not suppresses an enum's declaredClass property by default [eap-7.4.z] (CVE-2025-48734)
- hibernate-validator: Hibernate Validator Expression Language Injection [eap-7.4.z] (CVE-2025-35036)
- org.wildfly.core/wildfly-core-management-subsystem: Wildfly vulnerable to Cross-Site Scripting (XSS) [eap-7.4.z] (CVE-2024-10234)
- org.apache.cxf/cxf-core: Apache CXF: Denial of Service vulnerability with temporary files [eap-7.4.z] (CVE-2025-23184)
- org.jboss.hal-hal-parent: Stored Cross-Site Scripting (XSS) in JBoss EAP Management Console [eap-7.4.z] (CVE-2025-2901)
- wildfly-ejb3: Improper Deserialization in JBoss Marshalling Allows Remote Code Execution [eap-7.4.z] (CVE-2025-2251)

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 7.4 for RHEL 9 x86_64

Fixes

- BZ - 2320848 - CVE-2024-10234 wildfly: Wildfly vulnerable to Cross-Site Scripting (XSS)
- BZ - 2339095 - CVE-2025-23184 org.apache.cxf: Apache CXF: Denial of Service vulnerability with temporary files
- BZ - 2351678 - CVE-2025-2251 org.jboss.eap:wildfly-ejb3: Improper Deserialization in JBoss Marshalling Allows Remote Code Execution
- BZ - 2355685 - CVE-2025-2901 org.jboss.hal-hal-parent: Stored Cross-Site Scripting (XSS) in JBoss EAP Management Console

- BZ - 2368956 - CVE-2025-48734 commons-beanutils: Apache Commons BeanUtils: PropertyUtilsBean does not suppresses an enum's declaredClass property by default
- BZ - 2370118 - CVE-2025-35036 hibernate-validator: Hibernate Validator Expression Language Injection
- JBEAP-29219 - Tracker bug for the EAP 7.4.23 release for RHEL-9
- JBEAP-28676 - [GSS](7.4.z) Upgrade artemis from 2.16.0.redhat-00053 to 2.16.0.redhat-00055
- JBEAP-28905 - (7.4.z) Upgrade jbossws-cxf from 5.4.14.Final-redhat-00001 to 5.4.15.Final-redhat-00001
- JBEAP-29440 - [GSS](7.4.z) Upgrade Mojarra from 2.3.14.SP09-redhat-00001 to 2.3.14.SP10-redhat-00001
- JBEAP-29815 - (7.4.z) Upgrade wildfly-core from 15.0.42.Final-redhat-00001 to 15.0.43.Final-redhat-00001
- JBEAP-29862 - (7.4.z) Upgrade WildFly Elytron from 1.15.25.Final-redhat-00001 to 1.15.26.Final-redhat-00001
- JBEAP-29866 - (7.4.z) Upgrade Elytron Web from 1.9.4.Final-redhat-00001 to 1.9.6.Final-redhat-00001
- JBEAP-29914 - [GSS](7.4.z) Upgrade ironjacamar from 1.5.19.Final to 1.5.21.Final
- JBEAP-29969 - [GSS](7.4.z) ENTMQBR-9658 / ARTEMIS-5382 - Merged cluster of JGroup will not lead to the AMQ cluster update
- JBEAP-30031 - [GSS](7.4.z) Upgrade HAL to 3.3.27
- JBEAP-30059 - [GSS](7.4.z) Upgrade migration tool to 1.10.0.Final-redhat-00042
- JBEAP-30264 - (7.4.z) Upgrade commons-beanutils from 1.9.4.redhat-00002 to 1.11.0.redhat-00001
- JBEAP-30359 - (7.4.z) Upgrade hibernate-validator to 6.0.23.SP2

CVEs

- CVE-2024-10234
- CVE-2025-2251
- CVE-2025-2901
- CVE-2025-23184
- CVE-2025-23366
- CVE-2025-35036
- CVE-2025-48734

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/.

Red Hat

Quick Links

Help

Site Info

Related Sites

Partial system outage

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility