Red Hat F

RHSA

:24-11-04

Overview

Updated P

Synop

Importa

Type/

Security

Red H

Identi

View a

Topic

A securi 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 8.0.4 serves as a replacement for Red Hat JBoss Enterprise Application Platform 8.0.3, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 8.0.4 Release Notes for information about the most significant bug fixes and enhancements included in this release.

Security Fix(es):

- org.apache.cxf/cxf-rt-transports-http: unrestricted memory consumption in CXF HTTP clients [eap-8.0.z] (CVE-2024-41172)
- com.nimbusds/nimbus-jose-jwt: large JWE p2c header value causes Denial of Service [eap-8.0.z] (CVE-2023-52428)
- wildfly-domain-http: wildfly: No timeout for EAP management interface may lead to Denial of Service (DoS) [eap-8.0.z] (CVE-2024-4029)
- xalan: OpenJDK: integer truncation issue in Xalan-J (JAXP, 8285407) [eap-8.0.z] (CVE-2022-34169)
- org.keycloak/keycloak-services: Vulnerable Redirect URI Validation Results in Open Redirec [eap-8.0.z] (CVE-2024-8883)
- org.keycloak/keycloak-saml-core-public: Improper Verification of SAML Responses Leading to Privilege Escalation in Keycloak [eap-8.0.z] (CVE-2024-8698)
- org.keycloak/keycloak-saml-core: Improper Verification of SAML Responses Leading to Privilege Escalation in Keycloak [eap-8.0.z] (CVE-2024-8698)

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 8.0 for RHEL 8 x86_64

Fixes

- BZ - 2108554 - CVE-2022-34169 OpenJDK: integer truncation issue in Xalan-J (JAXP, 8285407)

- BZ - 2278615 - CVE-2024-4029 wildfly: No timeout for EAP management interface may lead to Denial of Service (DoS)
- BZ - 2298829 - CVE-2024-41172 apache: cxf: org.apache.cxf:cxf-rt-transports-http: unrestricted memory consumption in CXF HTTP clients
- BZ - 2309764 - CVE-2023-52428 nimbus-jose-jwt: large JWE p2c header value causes Denial of Service
- BZ - 2311641 - CVE-2024-8698 keycloak-saml-core: Improper Verification of SAML Responses Leading to Privilege Escalation in Keycloak
- BZ - 2312511 - CVE-2024-8883 Keycloak: Vulnerable Redirect URI Validation Results in Open Redirec
- JBEAP-27247 - Tracker bug for the EAP 8.0.4 release for RHEL-8
- JBEAP-24945 - (8.0.z) Upgrade to AMQ 7.12.x
- JBEAP-25035 - (8.0.z) Upgrade wildfly-artemis-integration to 2.0.2.Final-redhat-00001
- JBEAP-27002 - (8.0.z) Unable to update EAP from server zip (8.0.1+) with eap installation manager
- JBEAP-27194 - (8.0.z) Upgrade EAP Installer in EAP 8.0 Update 4
- JBEAP-27276 - (8.0.z) Upgrade Byteman from 4.0.20 to 4.0.23
- JBEAP-27293 - [PM](8.0.z) Upgrade Jandex to 3.0.8.redhat-00001 that supports SE 21
- JBEAP-27392 - [GSS](8.0.z) Upgrade Hibernate from 6.2.26.Final to 6.2.31.Final
- JBEAP-27543 - (8.0.z) Upgrade WildFly Core from 21.0.10.Final-redhat-00001 to 21.0.11.Final-redhat-00001 in EAP 8.0 Update 4
- JBEAP-27585 - (8.0.z) Upgrade EAP codebase to 8.0.6.GA-redhat-SNAPSHOT in EAP 8.0 update
- JBEAP-27643 - (8.0.z) Update Narayana to 6.0.3.Final
- JBEAP-27659 - [GSS](8.0.z) Upgrade insights java client from 1.1.2.redhat-00001 to 1.1.3.redhat-00001
- JBEAP-27688 - (8.0.z) Upgrade apache-cxf from 4.0.4 to 4.0.5
- JBEAP-27694 - (8.0.z) Upgrade JSTL Implementation from 3.0.0.redhat-00002 to 3.0.1.redhat-00001
- JBEAP-27957 - (8.0.z) Upgrade nimbus-jose-jwt from 9.24.4.redhat-00001 to 9.37.3
- JBEAP-28057 - (8.0.z) Update Keycloak from 22.0.11.redhat-00002 to 24.0.8
- JBEAP-28278 - (8.0.z) Upgrade EAP codebase to 8.0.6.SP1-redhat-SNAPSHOT in EAP 8.0 update 4
- JBEAP-28289 - (8.0.z) Upgrade artemis-wildfly-integration to 2.0.1

CVEs

- CVE-2022-34169
- CVE-2023-52428
- CVE-2024-4029
- CVE-2024-8698
- CVE-2024-8883

- CVE-2024-41172

References

- https://access.redhat.com/security/updates/classification/#important
- https://access.redhat.com/documentation/en-us/red_hat_jboss_enterprise_application_platform/8.0/

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