RHSA-2024:2945 - Security Advisory

Issued: 2024-05-21 Updated: 2024-05-21

Overview

Synopsis

Important: Red Hat AMQ Broker 7.12.0 release and security update

Type/Severity

Security Advisory: Important

Topic

Red Hat AMQ Broker 7.12.0 is now available from the Red Hat Customer Portal.

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

AMQ Broker is a high-performance messaging implementation based on ActiveMQ Artemis. It uses an asynchronous journal for fast message persistence, and supports multiple languages, protocols, and platforms.

This release of Red Hat AMQ Broker 7.12.0 includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Security Fix(es):

- (CVE-2023-6717) keycloak: XSS via assertion consumer service URL in SAML POST-binding flow
- (CVE-2024-1132) keycloak: path transversal in redirection validation
- (CVE-2024-1249) keycloak: org.keycloak.protocol.oidc: unvalidated cross-origin messages in checkLoginIframe leads to DDoS
- (CVE-2024-22259) springframework: URL Parsing with Host Validation
- (CVE-2022-41678) Apache ActiveMQ: Deserialization vulnerability on Jolokia that allows authenticated users to perform RCE
- (CVE-2023-44981) zookeeper: Authorization Bypass in Apache ZooKeeper
- (CVE-2023-6378) logback: serialization vulnerability in logback receiver
- (CVE-2023-6481) logback: A serialization vulnerability in logback receiver
- (CVE-2024-29025) netty-codec-http: Allocation of Resources Without Limits or Throttling
- (CVE-2024-29131) commons-configuration: StackOverflowError adding property in AbstractListDelimiterHandler.flattenIterator()
- (CVE-2024-29133) commons-configuration: StackOverflowError calling ListDelimiterHandler.flatten(Object, int) with a cyclical object tree

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

Solution

Before applying the update, back up your existing installation, including all applications, configuration files, databases and database settings.

The References section of this erratum contains a download link (you must log in to download the update).

Affected Products

- Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64

Fixes

- BZ - 2243436 - CVE-2023-44981 zookeeper: Authorization Bypass in Apache ZooKeeper
- BZ - 2252185 - CVE-2022-41678 Apache ActiveMQ: Deserialization vulnerability on Jolokia that allows authenticated users to perform RCE
- BZ - 2252230 - CVE-2023-6378 logback: serialization vulnerability in logback receiver
- BZ - 2252956 - CVE-2023-6481 logback: A serialization vulnerability in logback receiver
- BZ - 2253952 - CVE-2023-6717 keycloak: XSS via assertion consumer service URL in SAML POST-binding flow
- BZ - 2262117 - CVE-2024-1132 keycloak: path transversal in redirection validation
- BZ - 2262918 - CVE-2024-1249 keycloak: org.keycloak.protocol.oidc: unvalidated cross-origin messages in checkLoginIframe leads to DDoS

- BZ - 2269846 - CVE-2024-22259 springframework: URL Parsing with Host Validation
- BZ - 2270673 - CVE-2024-29133 commons-configuration: StackOverflowError calling ListDelimiterHandler.flatten(Object, int) with a cyclical object tree
- BZ - 2270674 - CVE-2024-29131 commons-configuration: StackOverflowError adding property in AbstractListDelimiterHandler.flattenIterator()
- BZ - 2272907 - CVE-2024-29025 netty-codec-http: Allocation of Resources Without Limits or Throttling

CVEs

- CVE-2022-41678
- CVE-2023-6378
- CVE-2023-6481
- CVE-2023-6717
- CVE-2023-44981
- CVE-2024-1132
- CVE-2024-1249
- CVE-2024-22259
- CVE-2024-29025
- CVE-2024-29131
- CVE-2024-29133

References

- https://access.redhat.com/security/updates/classification/#important
- https://access.redhat.com/jbossnetwork/restricted/listSoftware.html?downloadType=distributions&product=jboss.amq.broker&version=7.12.0
- https://access.redhat.com/documentation/en-us/red_hat_amq_broker/7.12

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

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
Cookie Preferences and Opt-Out Rights