RHSA-2025:12511 - Security Advisory

Issued: 2025-08-01 Updated: 2025-08-01

Overview

Synopsis

Important: Streams for Apache Kafka 3.0.0 release and security update

Type/Severity

Security Advisory: Important

Topic

Streams for Apache Kafka 3.0.0 is now available from the Red Hat Customer Portal.

Red Hat Product Security has rated this update as having a security impact of Moderate. 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 Streams for Apache Kafka, based on the Apache Kafka project, offers a distributed backbone that allows microservices and other applications to share data with extremely high throughput and extremely low latency.

This release of Red Hat Streams for Apache Kafka 3.0.0 serves as a replacement for Red Hat Streams for Apache Kafka 2.9.0, and includes security and bug fixes, and enhancements.

Security Fix(es):

- Cruise Control: json-smart: Uncontrolled Resource Consumption vulnerability in json-smart (Resource Exhaustion) Security [amq-st-2] "(CVE-2023-1370)"
- Cruise Control, Drain Cleaner: io.netty:netty-handler: SslHandler doesn't

correctly validate packets which can lead to native crash when using native SSLEngine Security[amq-st-2] "(CVE-2025-24970)"

- Cruise Control, Drain Cleaner: netty: Denial of Service attack on windows app using Netty Security [amq-st-2] "(CVE-2025-25193)"

Cruise Control: kafka: Apache Kafka: SCRAM authentication vulnerable to replay attacks when used without encryption Security [amq-st-2] "(CVE-2024-56128)"

- Cruise Control: kafka-clients: privilege escalation to filesystem read-access via automatic ConfigProvider Security [amq-st-2] "(CVE-2024-31141)"
- Cruise Control, Operator: Jetty: Gzip Request Body Buffer Corruption

Security[amq-st-2]"(CVE-2024-13009)"

- Cruise Control: org.eclipse.jetty:jetty-http: jetty: Jetty URI parsing of invalid authority Security [amq-st-2] "(CVE-2024-6763)"
- Cruise Control: commons-beanutils: Apache Commons BeanUtils:

PropertyUtilsBean does not suppresses an enum's declaredClass property by default Security [amq-st-2] "(CVE-2025-48734)"

- Cruise Control, Kafka, Drain Cleaner, Console: commons-lang-library:

Uncontrolled recursion flaw in Apache Commons Lang library [amq-st-2] "(CVE-2025-48924)"

- Opetator, Bridge: io.quarkus:quarkus-vertx package: data leak vulnerability has been discovered in the io.quarkus: quarkus-vertx package[amq-st-2] "(CVE-2025-49574)"
- Kafka, Operator, Bridge, Cruise Control, Bridge: Connect2id Nimbus JOSE + JWT: Denial of service flaw [amq-st-2] "(CVE-2025-53864)"
- Drain Cleaner: io.quarkus:quarkus-resteasy: Memory Leak in Quarkus RESTEasy Classic When Client Requests Timeout [amq-st-2] "(CVE-2025-1634)"
- Drain Cleaner: netty: Denial of Service attack on windows app using Netty[amq-st-2] "(CVE-2024-47535)"

Solution

Before applying this update, make sure all previously released errata relevant to your system have been applied.

For details on how to apply this update, refer to:

https://access.redhat.com/articles/11258

Affected Products

- Red Hat JBoss Middleware 1 x86_64

Fixes

- BZ - 2188542 - CVE-2023-1370 json-smart: Uncontrolled Resource Consumption vulnerability in json-smart (Resource Exhaustion)
- BZ - 2318563 - CVE-2024-6763 org.eclipse.jetty:jetty-http: jetty: Jetty URI parsing of invalid authority
- BZ - 2325538 - CVE-2024-47535 netty: Denial of Service attack on windows app using Netty
- BZ - 2327264 - CVE-2024-31141 kafka-clients: privilege escalation to filesystem read-access via automatic ConfigProvider
- BZ - 2333013 - CVE-2024-56128 kafka: Apache Kafka: SCRAM authentication vulnerable to replay attacks when used without encryption
- 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
- BZ - 2347319 - CVE-2025-1634 io.quarkus:quarkus-resteasy: Memory Leak in Quarkus RESTEasy Classic When Client Requests Timeout
- BZ - 2365135 - CVE-2024-13009 jetty-server: Jetty: Gzip Request Body Buffer Corruption
- BZ - 2368956 - CVE-2025-48734 commons-beanutils: Apache Commons BeanUtils: PropertyUtilsBean does not suppresses an enum's declaredClass property by default
- BZ - 2374376 - CVE-2025-49574 io.quarkus/quarkus-vertx: Quarkus potential data leak
- BZ - 2379485 - CVE-2025-53864 com.nimbusds/nimbus-jose-jwt: Uncontrolled recursion in Connect2id Nimbus JOSE + JWT
- BZ - 2379554 - CVE-2025-48924 commons-lang/commons-lang: org.apache.commons/commons-lang3: Uncontrolled Recursion vulnerability in Apache Commons Lang
- ENTMQST-6772 - CVE-2025-49574 Data leak vulnerability in io.quarkus:quarkus-vertx package.
- ENTMQST-6773 - CVE-2025-53864 Denial of service flaw in Connect2id Nimbus JOSE + JWT

CVEs

- CVE-2023-1370
- CVE-2024-6763
- CVE-2024-13009
- CVE-2024-31141

- CVE-2024-47535
- CVE-2024-56128
- CVE-2025-1634
- CVE-2025-24970
- CVE-2025-25193
- CVE-2025-48734
- CVE-2025-48924
- CVE-2025-49574
- CVE-2025-53864

References

- https://access.redhat.com/security/updates/classification/#important

---

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