RHSA-2025:23417 - Security Advisory

Issued: 2025-12-16 Updated: 2025-12-16

Overview

Synopsis

Important: Streams for Apache Kafka 3.1.0 release and security update

Type/Severity

Security Advisory: Important

Topic

Streams for Apache Kafka 3.1.0 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 3.1.0 serves as a replacement for Red Hat Streams for Apache Kafka 3.0.1, and includes security and bug fixes, and enhancements.

Security Fix(es):

- Apache Kafka, Drain Cleaner, Bridge, Cruise Conreol, Proxy, Console: Netty's BrotliDecoder is vulnerable to DoS via zip bomb style attack"(CVE-2025-58057)"

- Apache Kafka, Proxy: Netty is vulnerable to request smuggling due to incorrect parsing of chunk extensions"(CVE-2025-58056)"
- Apache Kafka, Bridge, Drain Cleaner, Cruise Control, Console: Netty MadeYouReset HTTP/2 DDoS Vulnerability ("CVE-2025-55163")
- Apache Kafka: org.apache.commons:commons-lang3 : Uncontrolled Recursion("CVE-2025-48924")
- Drain Cleaner: io.quarkus:quarkus-resteasy: Memory Leak in Quarkus RESTEasy Classic When Client Requests Timeout("CVE-2025-1634")
- Drain Cleaner, Console: Data leak vulnerability in io.quarkus:quarkus-vertx package ("CVE-2025-49574")
- Cruise Control: org.apache.kafka/kafka_2.13: Apache Kafka: SCRAM authentication vulnerable to replay attacks when used without encryption (" CVE-2024-56128")
- Cruise Control: org.apache.kafka: Kafka Client Arbitrary File Read SSRF("CVE-2025-27817")
- Cruise Control: Kafka Clients Vulnerabiliy("CVE-2025-27819")
- Cruise Control: Kafka Clients Vulnerabiliy("CVE-2025-27818")
- Cruise Control, Console: io.vertx/vertx-core: Eclipse Vert.x Access Control Flaw ("CVE-2025-11965")
- Cruise Control, Console: Vertx - Cross-site scripting (XSS) vulnerability ("CVE-2025-11966")

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 - 2333013 - CVE-2024-56128 kafka: Apache Kafka: SCRAM authentication vulnerable to replay attacks when used without encryption
- BZ - 2347319 - CVE-2025-1634 io.quarkus:quarkus-resteasy: Memory Leak in Quarkus RESTEasy Classic When Client Requests Timeout
- BZ - 2371365 - CVE-2025-27819 org.apache.kafka: Kafka JNDI Login Module RCE Vulnerability
- BZ - 2371367 - CVE-2025-27817 org.apache.kafka: Kafka Client Arbitrary File Read SSRF
- BZ - 2371368 - CVE-2025-27818 apache-kafka: Apache Kafka: Possible RCE attack via SASL JAAS LdapLoginModule configuration
- BZ - 2374376 - CVE-2025-49574 io.quarkus/quarkus-vertx: Quarkus potential data leak

- BZ - 2379554 - CVE-2025-48924 commons-lang/commons-lang: org.apache.commons/commons-lang3: Uncontrolled Recursion vulnerability in Apache Commons Lang
- BZ - 2388252 - CVE-2025-55163 netty: netty-codec-http2: Netty MadeYouReset HTTP/2 DDoS Vulnerability
- BZ - 2392996 - CVE-2025-58056 netty-codec-http: Netty is vulnerable to request smuggling due to incorrect parsing of chunk extensions
- BZ - 2393000 - CVE-2025-58057 netty-codec: netty-codec-compression: Netty's BrotliDecoder is vulnerable to DoS via zip bomb style attack
- BZ - 2405789 - CVE-2025-11966 io.vertx/vertx-web: Eclipse Vert.x cross site scripting
- BZ - 2405820 - CVE-2025-11965 io.vertx/vertx-core: Eclipse Vert.x Access Control Flaw

CVEs

- CVE-2024-56128
- CVE-2025-1634
- CVE-2025-11965
- CVE-2025-11966
- CVE-2025-27817
- CVE-2025-27818
- CVE-2025-27819
- CVE-2025-48924
- CVE-2025-49574
- CVE-2025-55163
- CVE-2025-58056
- CVE-2025-58057

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/.