RHSA-2025:2416 - Security Advisory

Issued: 2025-03-05 Updated: 2025-03-05

Overview

Synopsis

Important: Streams for Apache Kafka 2.9.0 release and security update

Type/Severity

Security Advisory: Important

Topic

Streams for Apache Kafka 2.9.0 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 2.9.0 serves as a replacement for Red Hat Streams for Apache Kafka 2.8.0, and includes security and bug fixes, and enhancements.

Security Fix(es):

- Cruise Control:cio.netty:netty-common:4.1.115.Final-redhat [amq-st-2] "(CVE-2023-52428)"

- Cruise Control:com.nimbusds:nimbus-jose-jwt:9.37.2.redhat [amq-st-2] "(CVE-2024-47535)"
- Cruise Control:org.apache.kafka:kafka-clients:3.5.2.redhat+ [amq-st-2] "(CVE-2024-31141)"
- Cruise Control:io:commons-io:2.15.1.redhat+ [amq-st-2] "(CVE-2024-47554)"
- Cruise Control:org.eclipse.jetty:jetty-server:9.4.56.v20240826-redhat+ [amq-st-2] "(CVE-2024-8184)"
- Cruise Control:org.eclipse.jetty/jetty-server: Jetty ThreadLimitHandler.getRemote() vulnerable to remote DoS attacks [amq-st-2] "(CVE-2024-8184)"
- Kafka Exporter:golang-github-danielqsj-kafka_exporter: Golang FIPS zeroed buffer [amq-st-2] "(CVE-2024-9355)"
- Kafka Exporter:golang-github-danielqsj-kafka_exporter: net/http: Denial of service due to improper 100-continue handling in net/http [amq-st-2] "(CVE-2024-24791)"

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 AMQ Streams 2 for RHEL 9 x86_64
- Red Hat AMQ Streams 2 for RHEL 9 s390x
- Red Hat AMQ Streams 2 for RHEL 9 ppc64le
- Red Hat AMQ Streams 2 for RHEL 9 aarch64

Fixes

- BZ - 2295310 - CVE-2024-24791 net/http: Denial of service due to improper 100-continue handling in net/http
- BZ - 2309764 - CVE-2023-52428 nimbus-jose-jwt: large JWE p2c header value causes Denial of Service
- BZ - 2315719 - CVE-2024-9355 golang-fips: Golang FIPS zeroed buffer
- BZ - 2316271 - CVE-2024-47554 apache-commons-io: Possible denial of service attack on untrusted input to XmlStreamReader
- BZ - 2318564 - CVE-2024-8184 org.eclipse.jetty:jetty-server: jetty: Jetty ThreadLimitHandler.getRemote() vulnerable to remote DoS attacks
- 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

CVEs

- CVE-2023-52428
- CVE-2024-8184
- CVE-2024-9355
- CVE-2024-24791
- CVE-2024-31141
- CVE-2024-47535
- CVE-2024-47554

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/.