



Red Hat Product Errata RHSA-2025:9922 - Security Advisory

RHSA-2025:9922 - Security Advisory

Issued: 2025-06-30 Updated: 2025-06-30

[Overview](#)

Synopsis

Important: Streams for Apache Kafka 2.9.1 release and security update

Type/Severity

Security Advisory: Important

Topic

Streams for Apache Kafka 2.9.1 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 2.9.1 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, Bridge, Kafka: o.netty:netty-handler: SslHandler doesn't correctly validate packets which can lead to native crash when using native SSL Engine Security [amq-st-2] "(CVE-2025-24970)"
- Cruise Control, Bridge, Kafka: 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, Operator: Jetty: Gzip Request Body Buffer Corruption Security [amq-st-2] "(CVE-2024-13009)"
- Cruise Control: kafka-clients: privilege escalation to filesystem read-access via automatic ConfigProvider Security [amq-st-2] "(CVE-2024-31141)"
- Cruise Control, Operator, Kafka: org.eclipse.jetty:jetty-http: [jetty](#): Jetty URI parsing of invalid authority Security [amq-st-2] "(CVE-2024-6763)"
- Zookeeper: netty: Denial of Service attack on windows app using Netty

Security [amq-st-2] "(CVE-2024-47535)"

- Zookeeper, Kafka: commons-beanutils: Apache Commons BeanUtils: PropertyUtilsBean does not suppresses an enum's declaredClass property by default Security [amq-st-2] "(CVE-2025-48734)"
- Bridge: org.apache.kafka: Kafka Client Arbitrary File Read SSRF Security [amq-st-2] "(CVE-2025-27817)"
- Bridge, Drain Cleaner: io.quarkus:quarkus-resteasy: Memory Leak in Quarkus RESTEasy Classic When Client Requests Timeout Security "(CVE-2025-1634)"

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 - 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 - 2371367](#)  - CVE-2025-27817 org.apache.kafka: Kafka Client Arbitrary File Read SSRF
- [ENTMQST-6736](#)  - CVE-2024-47535 Enetty: Denial of Service attack on windows app using Netty
- [ENTMQST-6737](#)  - CVE-2024-6763 org.eclipse.jetty:jetty-http: jetty: Jetty URI parsing of invalid authority
- [ENTMQST-6738](#)  - CVE-2023-1370 json-smart: Uncontrolled Resource Consumption vulnerability in json-smart (Resource Exhaustion)
- [ENTMQST-6739](#)  - CVE-2025-27817 org.apache.kafka: Kafka Client Arbitrary File Read SSRF
- [ENTMQST-6740](#)  - CVE-2025-25193 netty: Denial of Service attack on windows app using Netty
- [ENTMQST-6741](#)  - CVE-2025-24970 io.netty:netty-handler: SslHandler doesn't correctly validate packets which can lead to native crash when using native SSLEngine

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-2025-27817](#)
- [CVE-2025-48734](#)

References

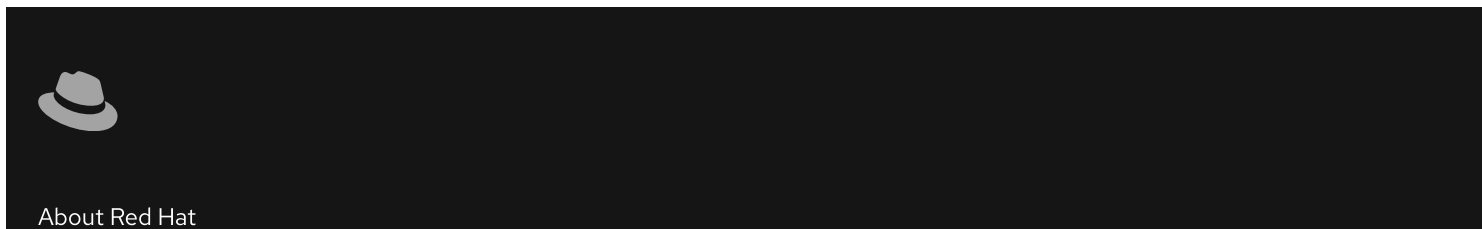
- <https://access.redhat.com/security/updates/classification/#important>

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



The image shows a dark-themed navigation bar for the Red Hat website. On the left is the Red Hat logo, which consists of a red fedora hat icon and the text "Red Hat" in white. On the right side of the bar are four social media icons: LinkedIn, YouTube, Facebook, and X. Below the bar is a vertical menu with four items: "Quick Links", "Help", "Site Info", and "Related Sites". Each item has a white downward-pointing chevron icon to its right, indicating that these are expandable sections.

✔ All systems operational



This section features a dark background with a small, light-colored icon of a fedora hat on the left. To the right of the icon, the text "About Red Hat" is displayed in a light color.

[Jobs](#)

[Events](#)

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

[© 2026 Red Hat](#)

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie Preferences and Opt-Out Rights](#)