



Red Hat F

RHSA Advis



1-06-24

Overview

Updated In

Synop

Importa

Type/Severity

Security Advisory: Important

Topic

Release of OpenShift Serverless Logic 1.33.0

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

This release includes security, bug fixes, and enhancements.

Security Fix(es):

- keycloak: org.keycloak.protocol.oidc: unvalidated cross-origin messages in checkLoginIframe leads to DDoS (CVE-2024-1249)
- keycloak: XSS via assertion consumer service URL in SAML POST-binding flow (CVE-2023-6717)

- pgjdbc: PostgreSQL JDBC Driver allows attacker to inject SQL if using PreferQueryMode=SIMPLE (CVE-2024-1597)
- camel-core: Exposure of sensitive data by crafting a malicious EventFactory (CVE-2024-22371)
- commons-compress: Denial of service caused by an infinite loop for a corrupted DUMP file (CVE-2024-25710)
- commons-compress: OutOfMemoryError unpacking broken Pack200 file (CVE-2024-26308)
- jose4j: denial of service via specially crafted JWE (CVE-2023-51775)

For more details about the security issues, including the impact, a CVSS score, acknowledgements, and other related information, refer to the CVE pages listed in the References section.

Solution

See the Red Hat OpenShift serverless 1.33 documentation at:

https://access.redhat.com/documentation/en-us/red_hat_openshift_serverless/1.33

Affected Products

- Red Hat OpenShift Serverless 1 for RHEL 8 x86_64
- Red Hat OpenShift Serverless for IBM Power, little endian 1 for RHEL 8 ppc64le
- Red Hat OpenShift Serverless for ARM 1 for RHEL 8 aarch64

Fixes

- [BZ - 2253952](#) - CVE-2023-6717 keycloak: XSS via assertion consumer service URL in SAML POST-binding flow
- [BZ - 2262918](#) - CVE-2024-1249 keycloak: org.keycloak.protocol.oidc: unvalidated cross-origin messages in checkLoginIframe leads to DDoS
- [BZ - 2264988](#) - CVE-2024-25710 commons-compress: Denial of service caused by an infinite loop for a corrupted DUMP file
- [BZ - 2264989](#) - CVE-2024-26308 commons-compress: OutOfMemoryError unpacking broken Pack200 file
- [BZ - 2266024](#) - CVE-2024-22371 camel-core: Exposure of sensitive data by crafting a malicious EventFactory
- [BZ - 2266523](#) - CVE-2024-1597 pgjdbc: PostgreSQL JDBC Driver allows attacker to inject SQL if using PreferQueryMode=SIMPLE
- [BZ - 2266921](#) - CVE-2023-51775 jose4j: denial of service via specially crafted JWE

CVEs

- [CVE-2023-6717](#)
- [CVE-2023-51775](#)
- [CVE-2024-1249](#)

- [CVE-2024-1597](#)
- [CVE-2024-22371](#)
- [CVE-2024-25710](#)
- [CVE-2024-26308](#)

References

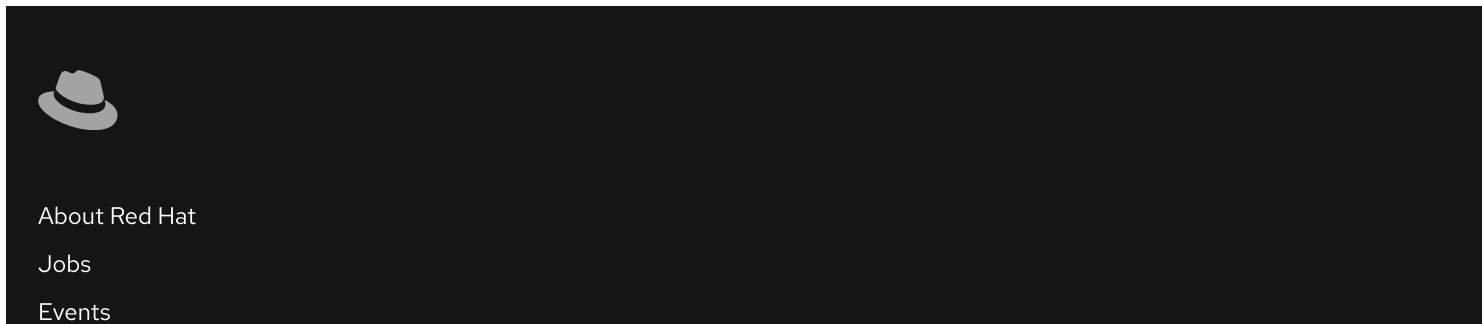
- <https://access.redhat.com/security/updates/classification/#important>
- https://access.redhat.com/documentation/en-us/red_hat_openshift_serverless/1.33

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



The image shows the Red Hat logo (a red hat) and the text "Red Hat" in white on a dark background. To the right of the logo are four social media icons: LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a navigation menu with four items: "Quick Links", "Help", "Site Info", and "Related Sites". Each item has a white downward-pointing chevron icon to its right. The menu items are separated by thin white horizontal lines.

✓ All systems operational



The image shows a footer navigation menu on a dark background. It starts with a small white hat icon. Below the icon are three links: "About Red Hat", "Jobs", and "Events", all in white text.

[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 Do Not Sell or Share My Personal Information](#)