



# RHSA-2024:1868 - Security Advisory

 Issued: 2024-04-16    Updated: 2024-04-16

Overview

## Synopsis

Important: Red Hat build of Keycloak security update

## Type/Severity

Security Advisory: Important

## Topic

An update is now available for Red Hat build of Keycloak.

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

Red Hat build of Keycloak 22.0.10 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications.

Security Fix(es):

- path transversal in redirection validation (CVE-2024-1132)
- org.keycloak.protocol.oidc: unvalidated cross-origin messages in checkLoginIframe leads to DDoS (CVE-2024-1249)
- secondary factor bypass in step-up authentication (CVE-2023-3597)
- Authorization Bypass (CVE-2023-6544)

- XSS via assertion consumer service URL in SAML POST-binding flow (CVE-2023-6717)
- session hijacking via re-authentication (CVE-2023-6787)
- impersonation via logout token exchange (CVE-2023-0657)
- Log Injection during WebAuthn authentication or registration (CVE-2023-6484)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

## 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 build of Keycloak Text-only Advisories x86\_64

## Fixes

- BZ - 2166728  - CVE-2023-0657 keycloak: impersonation via logout token exchange
- BZ - 2221760  - CVE-2023-3597 keycloak: secondary factor bypass in step-up authentication
- BZ - 2248423  - CVE-2023-6484 keycloak: Log Injection during WebAuthn authentication or registration
- BZ - 2253116  - CVE-2023-6544 keycloak: Authorization Bypass
- BZ - 2253952  - CVE-2023-6717 keycloak: XSS via assertion consumer service URL in SAML POST-binding flow
- BZ - 2254375  - CVE-2023-6787 keycloak: session hijacking via re-authentication
- BZ - 2262117  - CVE-2024-1132 keycloak: path transversal in redirection validation
- BZ - 2262918  - CVE-2024-1249 keycloak: org.keycloak.protocol.oidc: unvalidated cross-origin messages in checkLoginIframe leads to DDoS

## CVEs

- CVE-2023-0657 
- CVE-2023-3597 
- CVE-2023-6484 
- CVE-2023-6544 
- CVE-2023-6717 
- CVE-2023-6787 
- CVE-2024-1132 

- [CVE-2024-1249](#) 

## References

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

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



The navigation menu features the Red Hat logo on the left and social media icons for LinkedIn, YouTube, Facebook, and X on the right. Below these are four expandable menu items: Quick Links, Help, Site Info, and Related Sites, each with a downward-pointing chevron icon.

 All systems operational



The footer navigation menu includes a small hat icon and a list of links: About Red Hat, Jobs, Events, Locations, Contact Red Hat, Red Hat Blog, and 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](#)