Red Hat F

RHSA

4-04-16

Overview

Synop

Importa

Type/

Security

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. More contact details at https://access.redhat.com/security/team/contact/.

Cool Stuff Store

Red Hat Summit
