RHSA-2024:1867 - Security Advisory

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

Synopsis

Moderate: Red Hat build of Keycloak 22.0.10 enhancement and security update

Type/Severity

Security Advisory: Moderate

Topic

A bug update is now available for Red Hat build of Keycloak 22.0.10 images running on OpenShift Container Platform. This is an enhancement and security update with Moderate impact rating.

Description

Red Hat build of Keycloak 22.0.10 is an integrated solution, available as a Red Hat JBoss Middleware for OpenShift containerized image, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications.

Security Fix(es):

- Authorization Bypass (CVE-2023-6544)
- XSS via assertion consumer service URL in SAML POST-binding flow (CVE-2023-6717)
- path transversal in redirection validation (CVE-2024-1132)
- unvalidated cross-origin messages in checkLoginIframe leads to DDoS (CVE-2024-1249)
- path traversal in the redirect validation (CVE-2024-2419)
- secondary factor bypass in step-up authentication (CVE-2023-3597)

- impersonation via logout token exchange (CVE-2023-0657)
- session hijacking via re-authentication (CVE-2023-6787)
- keycloak-rhel9-operator-bundle-container: Log Injection during WebAuthn authentication or registration (CVE-2023-6484)
- keycloak-rhel9-operator-container: Log Injection during WebAuthn authentication or registration (CVE-2023-6484)

This erratum releases a bug update and enhancement images for Red Hat build of Keycloak 22.0.10 for use within the OpenShift Container Platform 4.12, 4.13, 4.14 and 4.15 cloud computing Platform-as-a-Service (PaaS) for on-premise or private cloud deployments, aligning with the standalone product release.

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
- BZ - 2269371 - CVE-2024-2419 keycloak: path traversal in the redirect validation

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
- CVE-2024-2419

References

- https://access.redhat.com/security/updates/classification/#moderate

---

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