



Red Hat Product Errata    RHSA-2024:6500 - Security Advisory

# RHSA-2024:6500 - Security Advisory

Issued: 2024-09-09    Updated: 2024-09-09

[Overview](#)[Updated Images](#)

## Synopsis

Moderate: Red Hat build of Keycloak 22.0.12 Images Update

## Type/Severity

Security Advisory: Moderate

## Topic

New images are available for Red Hat build of Keycloak 22.0.12 and Red Hat build of Keycloak 22.0.12 Operator, running on OpenShift Container Platform. This is a security update with Moderate impact rating.

## Description

Red Hat build of Keycloak is an integrated sign-on solution, available as a Red Hat JBoss Middleware for OpenShift containerized image. The Red Hat build of Keycloak for OpenShift image provides an authentication server that you can use to log in centrally, log out, and register. You can also manage user accounts for web applications, mobile applications, and RESTful web services.

Red Hat build of Keycloak Operator for OpenShift simplifies deployment and management of Keycloak 22.0.12 clusters.

This erratum releases new images for Red Hat build of Keycloak 22.0.12 for use within the OpenShift Container Platform cloud computing Platform-as-a-Service (PaaS) for on-premise or private cloud deployments, aligning with the standalone product release.

Security fixes:

- potential bypass of brute force protection (CVE-2024-4629)
- session fixation in elytron saml adapters (CVE-2024-7341)
- Leak of configured LDAP bind credentials through the Keycloak admin console (CVE-2024-5967)

## Solution

Before applying the update, back up your existing installation, including all applications, configuration files, databases and database settings, and so on.

## Affected Products

- Red Hat build of Keycloak Text-only Advisories x86\_64

## Fixes

- BZ - 2276761 [↗](#) - CVE-2024-4629 keycloak: potential bypass of brute force protection
- BZ - 2292200 [↗](#) - CVE-2024-5967 keycloak: Leak of configured LDAP bind credentials through the Keycloak admin console
- BZ - 2302064 [↗](#) - CVE-2024-7341 wildfly-elytron: org.keycloak/keycloak-services: session fixation in elytron saml adapters

## CVEs

- CVE-2024-4629 [↗](#)
- CVE-2024-5967 [↗](#)
- CVE-2024-7341 [↗](#)

## References

- <https://access.redhat.com/security/updates/classification/#moderate> [↗](#)

---

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



Quick Links



Help



Site Info



Related Sites



 Partial system outage



[About Red Hat](#)

[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