



Red Hat Product Errata    RHSA-2024:6499 - Security Advisory

# RHSA-2024:6499 - Security Advisory

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

[Overview](#)

## Synopsis

Moderate: Red Hat Single Sign-On 7.6.10 security update

## Type/Severity

Security Advisory: Moderate

## Topic

A security update is now available for Red Hat Single Sign-On 7.6 from the Customer Portal.

Red Hat Product Security has rated this update as having a security impact of Moderate. 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

<< AUTOMATICALLY GENERATED, EDIT PLEASE >>

Red Hat Single Sign-On 7.6 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications.

This release of Red Hat Single Sign-On 7.6.10 serves as a replacement for Red Hat Single Sign-On 7.6.9, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References.

Security Fix(es):

- 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)

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

## Solution

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

The References section of this erratum contains a download link (you must log in to download the update).

## Affected Products

- Red Hat Single Sign-On 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 and Opt-Out Rights