RHSA-2024:6495 - Security Advisory

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

Synopsis

Moderate: Red Hat Single Sign-On 7.6.10 security update on RHEL 9

Type/Severity

Security Advisory: Moderate

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

New Red Hat Single Sign-On 7.6.10 packages are now available for Red Hat Enterprise Linux 9.

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

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 on RHEL 9 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 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 Single Sign-On 7.6 for RHEL 9 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. More contact details at https://access.redhat.com/security/team/contact/.

Red Hat Summit
