

[Red Hat Product Errata](#)    [RHSA-2024:1862 - Security Advisory](#)

# RHSA-2024:1862 - Security Advisory

Issued: 2024-04-16

Updated: 2024-04-16

[Overview](#)[Updated Packages](#)

## Synopsis

Important: Red Hat Single Sign-On 7.6.8 security update on RHEL 9

## Type/Severity

Security Advisory: Important

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

## Topic

New Red Hat Single Sign-On 7.6.8 deliverables are now available for Red Hat Enterprise Linux 9.

This is an enhancement and security update with Important impact rating and package name 'rh-ssos7-keycloak'. 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 7.6.8 on RHEL 9 serves as a replacement for Red Hat Single Sign-On 7.6.7, and includes bug fixes, security updates and enhancements which are linked to in the References.

Security Fix(es):

- Authorization Bypass (CVE-2023-6544)
- Log Injection during WebAuthn authentication or registration (CVE-2023-6484)
- path transversal in redirection validation (CVE-2024-1132)
- unvalidated cross-origin messages in checkLoginIframe leads to DDoS (CVE-2024-1249)
- undertow: Out-of-memory Error after several closed connections with wildfly-http-client protocol (CVE-2024-1635)

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 - 2248423](#) - CVE-2023-6484 keycloak: Log Injection during WebAuthn authentication or registration
- [BZ - 2253116](#) - CVE-2023-6544 keycloak: Authorization Bypass
- [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 - 2264928](#) - CVE-2024-1635 undertow: Out-of-memory Error after several closed connections with wildfly-http-client protocol






## CVEs

- [CVE-2023-6484](#) 
- [CVE-2023-6544](#) 
- [CVE-2024-1132](#) 
- [CVE-2024-1249](#) 
- [CVE-2024-1635](#) 


## References

- <https://access.redhat.com/security/updates/classification/#important> 


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](#) 

---

 All systems operational



[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](#)