



Red Hat Product Errata    RHSA-2024:6880 - Security Advisory

# RHSA-2024:6880 - Security Advisory

Issued: 2024-09-19    Updated: 2024-09-19

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

## Synopsis

Important: Red Hat Single Sign-On 7.6.11 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 7.6.11 packages are now available for Red Hat Enterprise Linux 9.

Red Hat Product Security has rated this update as having a security impact of none. 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 7.6.11 on RHEL 9 serves as a replacement for Red Hat Single Sign-On 7.6.10, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References.

Security Fix(es):

- Improper Verification of SAML Responses Leading to Privilege Escalation in Keycloak (CVE-2024-8698)
- Vulnerable Redirect URI Validation Results in Open Redirec (CVE-2024-8883)

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 - 2311641  - CVE-2024-8698 keycloak-saml-core: Improper Verification of SAML Responses Leading to Privilege Escalation in Keycloak
- BZ - 2312511  - CVE-2024-8883 Keycloak: Vulnerable Redirect URI Validation Results in Open Redirec

## CVEs

- CVE-2024-8698 
- CVE-2024-8883 

## 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 

---

 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](#)