



红帽产品勘误      RHSA-2024:1866 - Security Advisory

## RHSA-2024:1866 - Security Advisory

发布：2024-04-16    已更新：2024-04-16

概述

### 概述

Important: Red Hat Single Sign-On 7.6.8 security update

### 类型/严重性

Security Advisory: Important

### 标题

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

This is an enhancement and security update with Important impact rating and package name 'rh-sso7-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.

### 描述

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 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.

## 解决方案

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).

## 受影响的产品

- Red Hat Single Sign-On Text-Only Advisories x86\_64

## 修复

- [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

## CVE

- [CVE-2023-3597](#)
- [CVE-2023-6484](#)
- [CVE-2023-6544](#)
- [CVE-2024-1132](#)
- [CVE-2024-1249](#)
- [CVE-2024-1635](#)

## 参考

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

Red Hat 安全团队联络方式为 [secalert@redhat.com](mailto:secalert@redhat.com)。更多联络细节请参考 <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](#)