

[Red Hat Product Errata](#) [RHSA-2024:1864 - Security Advisory](#)

RHSA-2024:1864 - Security Advisory

Issued: 2024-04-16 Updated: 2024-04-16[Overview](#)[Updated Images](#)

Synopsis

Important: Red Hat Single Sign-On 7.6.8 for OpenShift image enhancement and security update

Type/Severity

Security Advisory: Important

Topic

A new image is available for Red Hat Single Sign-On 7.6.8, running on OpenShift Container Platform 3.10 and 3.11, and 4.3.

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.

Description

Red Hat Single Sign-On is an integrated sign-on solution, available as a Red Hat JBoss Middleware for OpenShift containerized image. The Red Hat Single Sign-On for OpenShift image provides an authentication server that you can use to log in centrally, log out, and register. You can also manage user accounts for web applications, mobile applications, and RESTful web services.

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)

This erratum releases a new image for Red Hat Single Sign-On 7.6.8 for use within the OpenShift Container Platform 3.10, OpenShift Container Platform 3.11, and within the OpenShift Container Platform 4.3 cloud computing Platform-as-a-Service (PaaS) for on-premise or private cloud deployments, aligning with the standalone product release.

Solution

To update to the latest Red Hat Single Sign-On 7.6.8 for OpenShift image, Follow these steps to pull in the content:

1. On your main hosts, ensure you are logged into the CLI as a cluster administrator or user with project administrator access to the global "openshift" project. For example:

```
$ oc login -u system:admin
```

2. Update the core set of Red Hat Single Sign-On resources for OpenShift in the "openshift" project by running the following commands:

```
$ for resource in sso76-image-stream.json \  
sso76-https.json \  
sso76-mysql.json \  
sso76-mysql-persistent.json \  
sso76-postgresql.json \  
sso76-postgresql-persistent.json \  
sso76-x509-https.json \  
sso76-x509-mysql-persistent.json \  
sso76-x509-postgresql-persistent.json  
do  
oc replace -n openshift --force -f \  
https://raw.githubusercontent.com/jboss-container-images/redhat-sso-7-openshift-  
image/v7.6.8.GA/templates/${resource}  
done
```

3. Install the Red Hat Single Sign-On 7.6.8 for OpenShift streams in the "openshift" project by running the following commands:

```
$ oc -n openshift import-image redhat-sso76-openshift:1.0
```

Affected Products

- Red Hat OpenShift Container Platform 4.12 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform 4.11 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.10 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for Power 4.9 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.10 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.9 for RHEL 8 s390x

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-2021-43618 [↗](#)
- CVE-2023-4408 [↗](#)
- CVE-2023-6484 [↗](#)
- CVE-2023-6544 [↗](#)
- CVE-2023-28322 [↗](#)
- CVE-2023-38546 [↗](#)
- CVE-2023-46218 [↗](#)
- CVE-2023-50387 [↗](#)
- CVE-2023-50868 [↗](#)
- CVE-2023-52425 [↗](#)
- CVE-2024-1132 [↗](#)
- CVE-2024-1249 [↗](#)
- CVE-2024-1635 [↗](#)
- CVE-2024-28834 [↗](#)


References

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

The Red Hat security contact is secalert@redhat.com. More contact details at <https://access.redhat.com/security/team/contact/>.



The navigation menu features the Red Hat logo on the left and social media icons for LinkedIn, YouTube, Facebook, and X on the right. Below these are four main menu items: 'Quick Links', 'Help', 'Site Info', and 'Related Sites', each with a downward-pointing chevron icon to its right.

 Partial system outage



The footer menu is located in the bottom left corner and includes a small hat icon. It lists several links: 'About Red Hat', 'Jobs', 'Events', 'Locations', 'Contact Red Hat', 'Red Hat Blog', 'Inclusion at Red Hat', and '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](#)