



Red Hat Product Errata RHSA-2024:6497 - Security Advisory

RHSA-2024:6497 - Security Advisory

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

[Overview](#)

[Updated Images](#)

Synopsis

Moderate: Red Hat Single Sign-On 7.6.10 for OpenShift image enhancement update

Type/Severity

Security Advisory: Moderate

Topic

A new image is available for Red Hat Single Sign-On 7.6.10, running on OpenShift Container Platform 3.10 and 3.11, and 4.3. This is a security update with Moderate impact rating.

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.

This erratum releases a new image for Red Hat Single Sign-On 7.6.10 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.

Security fixes:

- 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)

Solution

To update to the latest Red Hat Single Sign-On 7.6.10 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/v7.6.10.GA/templates/\${resource}  
done
```




3. Install the Red Hat Single Sign-On 7.6.10 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 - 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-2024-1737](#) 
- [CVE-2024-1975](#) 
- [CVE-2024-2398](#) 
- [CVE-2024-4629](#) 
- [CVE-2024-5967](#) 
- [CVE-2024-6345](#) 
- [CVE-2024-7341](#) 
- [CVE-2024-37370](#) 
- [CVE-2024-37371](#) 
- [CVE-2024-37891](#) 

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/>.



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