



About cookies on this site



红帽产品

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

RHSA Advis

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

4-09-19

概述

更新的镜像

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for

概述

Important

Accept Default

Do Not Sell or Share My Personal Information

类型/严重性

Security Advisory: Important [Cookie Preferences](#) | [Privacy Statement](#)

标题

A new image is available for Red Hat Single Sign-On 7.6.11, running on OpenShift Container Platform 3.10 and 3.11, and 4.3.

描述

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):

- 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)

This erratum releases a new image for Red Hat Single Sign-On 7.6.11 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.

解决方案

To update to the latest Red Hat Single Sign-On 7.6.11 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/v7.6.11.GA/templates/\${resource}  
done
```

3. Install the Red Hat Single Sign-On 7.6.11 for OpenShift streams in the "openshift" project by running the following commands:

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

受影响的产品

- 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

修复

- [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

CVE

- [CVE-2024-8698](#)
- [CVE-2024-8883](#)

参考

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

Red Hat 安全团队联络方式为 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



 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 and Do Not Sell or Share My Personal Information](#)