



红帽产品

# RHSA Advis



.-09-09

概述

更新的软件

## 概述

Moderat

## 类型/严重性

Security Advisory: Moderate

### Red Hat Lightspeed patch analysis

识别并修复受此公告影响的系统。

[查看受影响的系统](#)

## 标题

New Red Hat Single Sign-On 7.6.10 packages are now available for Red Hat Enterprise Linux 7.

Red Hat Product Security has rated this update as having a security impact of Moderate. 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 7.6.10 on RHEL 7 serves as a replacement for Red Hat Single Sign-On 7.6.9, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References.

Security Fix(es):

- 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)

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 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> 




## 受影响的产品

- Red Hat Single Sign-On 7.6 for RHEL 7 x86\_64

## 修复

- [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

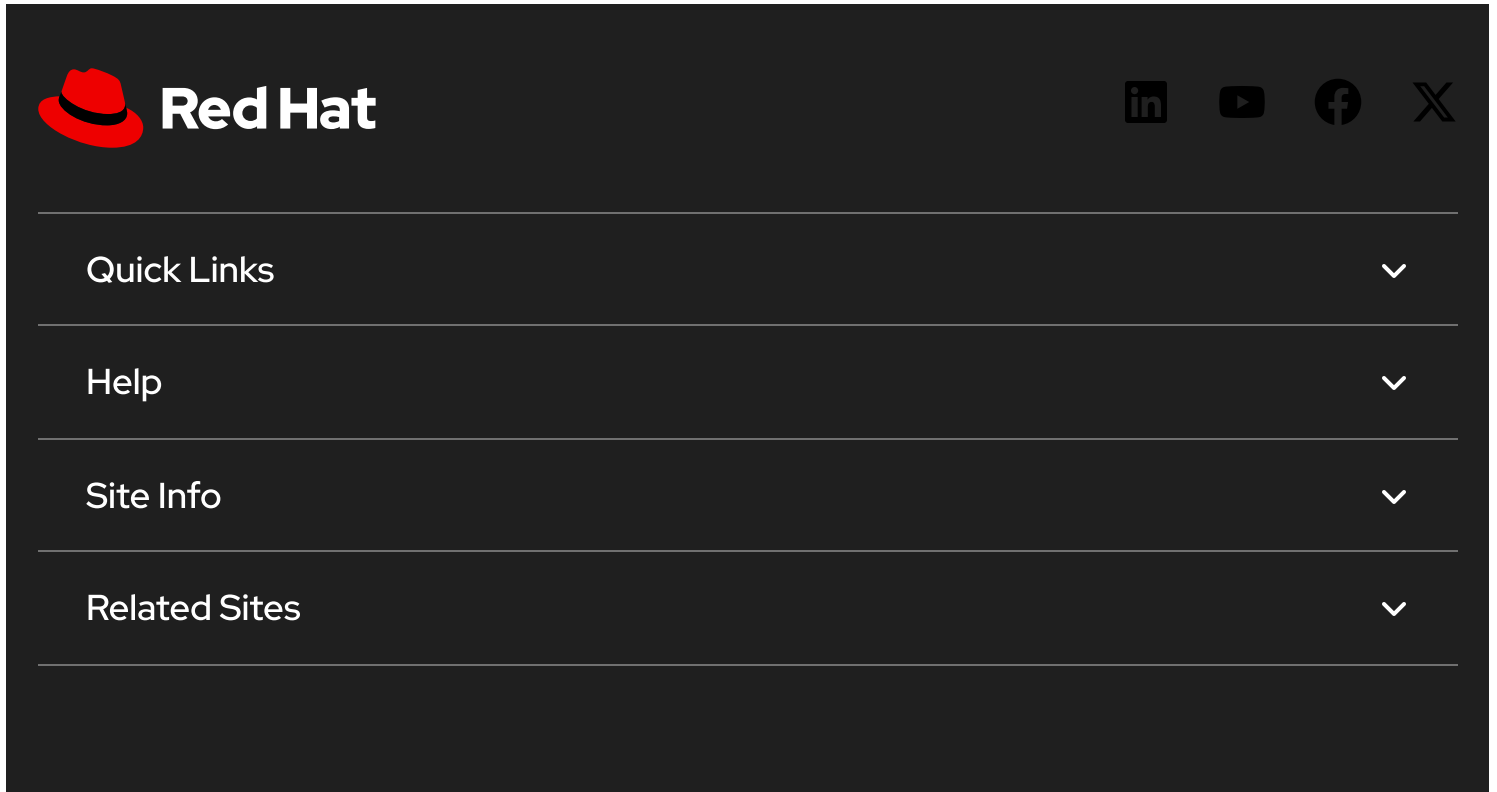
## CVE

- [CVE-2024-4629](#) 
- [CVE-2024-5967](#) 
- [CVE-2024-7341](#) 

## 参考

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

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/>。



The image shows a dark-themed navigation bar for Red Hat. On the left is the Red Hat logo (a red hat icon) and the text "Red Hat". On the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below the logo and text are four menu items: "Quick Links", "Help", "Site Info", and "Related Sites", each with a downward-pointing chevron icon to its right.

✔ All systems operational



The image shows a dark-themed footer menu. At the top left is a small grey hat icon. Below it is a list of 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 Do Not Sell or Share My Personal Information](#)