



Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site



Red Hat F

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

i-04-02

Overview

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.

Updated In

Synop

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 targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Importan

Type/

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Security

Topic

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

New ima

26.4.11

Operato

Descri

Red Hat

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser's global privacy preferences for web applications, mobile applications, and RESTful web services.

dleware

for Oper

ides an

authenti

manage

user accounts

for web applications, mobile applications, and RESTful web services. Red Hat build of Keycloak Operator for OpenShift simplifies deployment and management of Keycloak 26.4.11 clusters.

This erratum releases new images for Red Hat build of Keycloak 26.4.11 for use within the OpenShift Container Platform cloud computing Platform-as-a-Service (PaaS) for on-premise or private cloud deployments, aligning with the standalone product release.

Security fixes:

- Keycloak Admin REST API: Improper Access Control leads to sensitive role metadata information disclosure (CVE-2025-14082)
- Improper Access Control in Admin REST API leads to information disclosure (CVE-2025-14083)
- keycloak-rhel9-operator: Keycloak IDOR in realm client creating/deleting (CVE-2025-14777)
- Keycloak Refresh Token Reuse Bypass via TOCTOU Race Condition (CVE-2026-1035)
- Blind Server-Side Request Forgery (SSRF) in Keycloak OIDC Dynamic Client Registration via jwks_uri (CVE-2026-1180)
- Information Disclosure via improper role enforcement in UMA 2.0 Protection API (CVE-2026-3190)
- Privilege escalation via manage-clients permission (CVE-2026-3121)
- Information disclosure due to redirect_uri validation bypass (CVE-2026-3872)
- Information disclosure of disabled user attributes via administrative endpoint (CVE-2026-3911)
- Improper Access Control Leading to MFA Deletion and Account Takeover in Keycloak Account REST API (CVE-2026-3429)
- Information disclosure via authorization bypass in Admin API (CVE-2026-2366)
- Replay of action tokens via improper handling of single-use entries (CVE-2026-4325)
- UMA policy bypass allows authenticated users to gain unauthorized access to victim-owned resources (CVE-2026-4636)
- Privilege escalation via forged authorization codes due to SingleUseObjectProvider isolation flaw (CVE-2026-4282)
- Denial of Service via excessive processing of OpenID Connect scope parameters (CVE-2026-4634)

Solution

Before applying the update, back up your existing installation, including all applications, configuration files, databases and database settings, and so on.





Affected Products

- Red Hat build of Keycloak Text-only Advisories x86_64

Fixes

(none)

CVEs

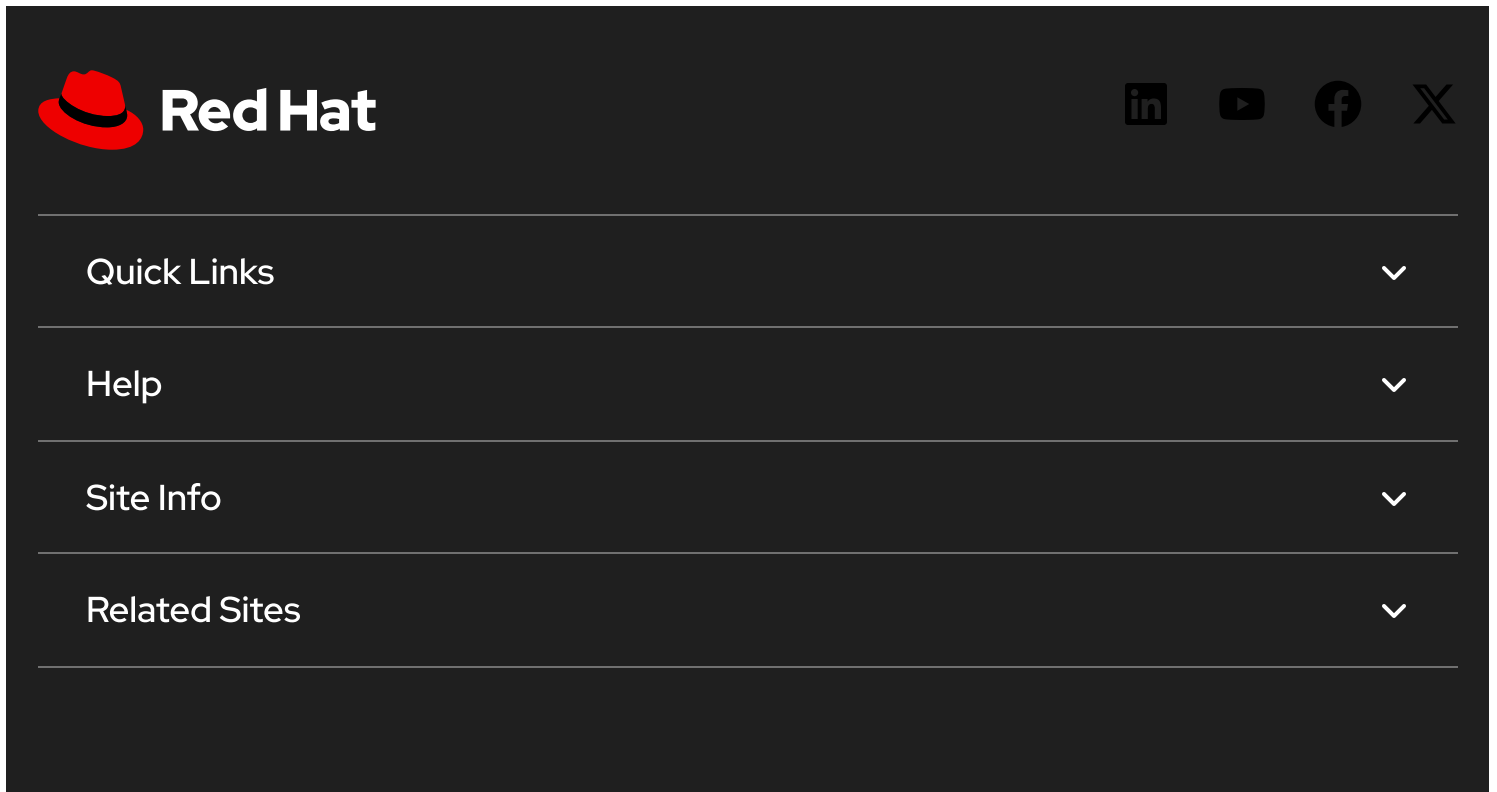
- [CVE-2025-14082](#) 
- [CVE-2025-14083](#) 
- [CVE-2025-14777](#) 
- [CVE-2026-1035](#) 

- [CVE-2026-1180](#)
- [CVE-2026-2366](#)
- [CVE-2026-3121](#)
- [CVE-2026-3190](#)
- [CVE-2026-3429](#)
- [CVE-2026-3872](#)
- [CVE-2026-3911](#)
- [CVE-2026-4282](#)
- [CVE-2026-4325](#)
- [CVE-2026-4634](#)
- [CVE-2026-4636](#)


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

 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](#)