RHSA-2026:6478 - Security Advisory

Issued: 2026-04-02 Updated: 2026-04-02

Overview

Updated Images

Synopsis

Important: Red Hat build of Keycloak 26.4.11 Images Update

Type/Severity

Security Advisory: Important

Topic

New images are available for Red Hat build of Keycloak 26.4.11 and Red Hat build of Keycloak 26.4.11 Operator, running on OpenShift Container Platform

Description

Red Hat build of Keycloak is an integrated sign-on solution, available as a Red Hat JBoss Middleware for OpenShift containerized image. The Red Hat build of Keycloak 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.
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/.

Red Hat

Quick Links

Help

Site Info

Related Sites

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