

[Red Hat Product Errata](#)    [RHSA-2024:10175 - Security Advisory](#)

## RHSA-2024:10175 - Security Advisory

Issued: 2024-11-21    Updated: 2024-11-21

[Overview](#)[Updated Images](#)

### Synopsis

Important: Red Hat build of Keycloak 24.0.9 Images Update

### Type/Severity

Security Advisory: Important

### Topic

New images with security impact Important are available for Red Hat build of Keycloak 24.0.9 and Red Hat build of Keycloak 24.0.9 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 24.0.9 clusters.

This erratum releases new images for Red Hat build of Keycloak 24.0.9 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:

- Sensitive Data Exposure in Keycloak Build Process (CVE-2024-10451)
- Keycloak Denial of Service (CVE-2024-10270)
- Keycloak path traversal (CVE-2024-10492)
- Keycloak proxy header handling Denial-of-Service (DoS) vulnerability (CVE-2024-9666)
- Keycloak TLS passthrough (CVE-2024-10039)

## Solution

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> 






## Affected Products

- Red Hat build of Keycloak Text-only Advisories x86\_64

## Fixes

- [BZ - 2317440](#)  - CVE-2024-9666 org.keycloak/keycloak-quarkus-server: Keycloak proxy header handling Denial-of-Service (DoS) vulnerability
- [BZ - 2319217](#)  - CVE-2024-10039 keycloak-core: mTLS passthrough
- [BZ - 2321214](#)  - CVE-2024-10270 org.keycloak:keycloak-services: Keycloak Denial of Service
- [BZ - 2322096](#)  - CVE-2024-10451 org.keycloak:keycloak-quarkus-server: Sensitive Data Exposure in Keycloak Build Process
- [BZ - 2322447](#)  - CVE-2024-10492 keycloak-quarkus-server: Keycloak path traversal

## CVEs

- [CVE-2024-9666](#) 
- [CVE-2024-10039](#) 
- [CVE-2024-10270](#) 
- [CVE-2024-10451](#) 
- [CVE-2024-10492](#) 

## References

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

---

The Red Hat security contact is [secalert@redhat.com](mailto: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 and Do Not Sell or Share My Personal Information