Duplicate Advisory: Keycloak Session Fixation vulnerability

High severity GitHub Reviewed Published on Sep 9, 2024 to the GitHub Advisory Database • Updated on Dec 20, 2024

Withdrawn This advisory was withdrawn on Dec 20, 2024

Vulnerability details Dependabot alerts 0

Package

org.keycloak:keycloak-services (Maven)

Affected versions	Patched versions
< 22.0.12	22.0.12
>= 23.0.0, < 24.0.7	24.0.7
>= 25.0.0, < 25.0.5	25.0.5

Description

Duplicate Advisory

This advisory has been withdrawn because it is a duplicate of GHSA-5rxp-2rhr-qwqv. This link is maintained to preserve external references.

Original Description

A session fixation issue was discovered in the SAML adapters provided by Keycloak. The session ID and JSESSIONID cookie are not changed at login time, even when `the turnOffChangeSessionIdOnLogin` option is configured. This flaw allows an attacker who hijacks the current session before authentication to trigger session fixation.

References

- https://nvd.nist.gov/vuln/detail/CVE-2024-7341

- https://access.redhat.com/errata/RHSA-2024:6493
- https://access.redhat.com/errata/RHSA-2024:6494
- https://access.redhat.com/errata/RHSA-2024:6495
- https://access.redhat.com/errata/RHSA-2024:6497
- https://access.redhat.com/errata/RHSA-2024:6499
- https://access.redhat.com/errata/RHSA-2024:6500
- https://access.redhat.com/errata/RHSA-2024:6501
- https://access.redhat.com/errata/RHSA-2024:6502
- https://access.redhat.com/errata/RHSA-2024:6503
- https://access.redhat.com/security/cve/CVE-2024-7341
- https://bugzilla.redhat.com/show_bug.cgi?id=2302064
- keycloak/keycloak@ `2341d6e`
- keycloak/keycloak@ `5b3de0c`
- keycloak/keycloak@ `5e06da2`

Published by the National Vulnerability Database on Sep 9, 2024

Published to the GitHub Advisory Database on Sep 9, 2024

Reviewed on Sep 9, 2024

Last updated on Dec 20, 2024

Withdrawn on Dec 20, 2024

Severity

High 7.5 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	Low
User interaction	Passive

Vulnerable System Impact Metrics

Confidentiality	High

Integrity	High
Availability	High
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

EPSS score

Weaknesses

▶ CWE-384

CVE ID

No known CVE

GHSA ID

GHSA-j76j-rqwj-jmvv

Source code

keycloak/keycloak

Credits

 **stianst** Analyst

This advisory has been edited. See History.

See something to contribute? Suggest improvements for this vulnerability.