



Org.keycloak.protocol.oidc: keycloak refresh token reuse bypass via toctou race condition

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-1035
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-21 06:15:46 UTC
Updated	2026-04-02 14:16:25 UTC
Description	A flaw was found in the Keycloak server during refresh token processing, specifically in the TokenManager class responsible for...

Risk And Classification

Primary CVSS: v3.1 3.1 LOW from secalert@redhat.com

CVSS: 3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N

EPSS: 0.000110000 probability, percentile 0.012280000 (date 2026-04-07)

Problem Types: CWE-367 | CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Keycloak 26.4	unaffected 26.4-14 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.4	unaffected 26.4.11-1 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.4	unaffected 26.4-14 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.4.11	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8	Not specified	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	Not specified	Not specified
CNA	Red Hat	Red Hat Single Sign-On 7	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:6478	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2026-1035	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2026:6477	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Mohamed Amine ait Ouchebou (mrecho) (Indiesecurity) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-01-16T06:45:27.223Z	Reported to Red Hat.
CNA	2026-01-21T00:00:00.000Z	Made public.

Workarounds

CNA: To mitigate this issue, configure the `refreshTokenMaxReuse` policy in Keycloak to a

CNA: To mitigate this issue, configure the `refreshTokenMaxReuse` policy in Keycloak to a value greater than zero. This prevents the race condition by allowing a limited number of reuses for refresh tokens, thereby maintaining the integrity of the Refresh Token Rotation hardening measure. Consult Keycloak documentation for specific configuration instructions. Changes to Keycloak configuration typically require a service restart or redeployment to take effect.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)