



# Keycloak: keycloak: information disclosure due to redirect\_uri validation bypass

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

## Summary

<b>CVE</b>	CVE-2026-3872
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-02 13:16:26 UTC
<b>Updated</b>	2026-04-16 20:52:42 UTC
<b>Description</b>	A flaw was found in Keycloak. This issue allows an attacker, who controls another path on the same web server, to bypass

## Risk And Classification

**Primary CVSS:** v3.1 7.3 HIGH from secalert@redhat.com

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

**EPSS:** 0.000330000 probability, percentile 0.094690000 (date 2026-04-16)

**Problem Types:** CWE-601 | CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Build Of Keycloak	-	All	All	All
Application	Redhat	Build Of Keycloak	26.2	All	All	All
Application	Redhat	Build Of Keycloak	26.2.15	All	All	All
Application	Redhat	Build Of Keycloak	26.4	All	All	All
Application	Redhat	Build Of Keycloak	26.4.11	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2.15-1 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2-18 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2-18 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2.15	Not specified	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	unaffected 26.4-14 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.4.11	Not specified	Not specified

### References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:6478	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:6476	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/errata/RHSA-2026:6475	secalert@redhat.com	access.redhat.com	Vendor Advisory
access.redhat.com/security/cve/CVE-2026-3872	secalert@redhat.com	access.redhat.com	Vendor Advisory
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Vendor Advisory
access.redhat.com/errata/RHSA-2026:6477	secalert@redhat.com	access.redhat.com	Vendor Advisory
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 Meeranh for reporting this issue. (en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-03-10T09:16:29.034Z	Reported to Red Hat.
CNA	2026-04-02T12:30:00.000Z	Made public.

### Workarounds

**CNA:** To mitigate this vulnerability, avoid using wildcards in `redirect\_uri` configurations within Keycloak. Restricting `redirect\_uri` to explicit, fully qualified URIs prevents the bypass of validation logic. This configuration change may require a service restart or reload 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](#)