Keycloak: keycloak: information disclosure due to redirect_uri validation bypass

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-3872
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-02 13:16:26 UTC
Updated	2026-04-16 20:52:42 UTC
Description	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

ntegrity

High

vailability

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.