Org.keycloak.protocol.oidc.grants: org.keycloak.services.managers: keycloak: server-side request forgery via oidc token endpoint manipulation

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-4874
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 08:16:22 UTC
Updated	2026-04-01 14:11:28 UTC
Description	A flaw was found in Keycloak. An authenticated attacker can perform Server-Side Request Forgery (SSRF) by manipulating

Risk And Classification

Primary CVSS: v3.1 3.1 LOW from nvd@nist.gov

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

EPSS: 0.000280000 probability, percentile 0.078590000 (date 2026-04-01)

Problem Types: CWE-918 | CWE-918 Server-Side Request Forgery (SSRF)

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/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	Jboss Enterprise Application Platform	8.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform Expansion Pack	-	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Keycloak	Not specified	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak	Not specified	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak	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
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Vendor Advisory
access.redhat.com/security/cve/CVE-2026-4874	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 Evan Hendra (Independent Security Researcher) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-26T05:51:10.233Z	Reported to Red Hat.
CNA	2026-03-26T05:56:03.440Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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