Keycloak-services: blind server-side request forgery (ssrf) via http redirect handling in keycloak

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-4366
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-18 04:17:32 UTC
Updated	2026-04-01 15:10:12 UTC
Description	A flaw was identified in Keycloak, an identity and access management solution, where it improperly follows HTTP redirects

Risk And Classification

Primary CVSS: v3.1 5.8 MEDIUM from secalert@redhat.com

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

EPSS: 0.000370000 probability, percentile 0.109620000 (date 2026-04-01)

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

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	5.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N
3.1	CNA	CVSS	5.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

Low

ntegrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/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
access.redhat.com/security/cve/CVE-2026-4366	secalert@redhat.com	access.redhat.com	Vendor Advisory
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, 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 Georgije Vukov (Elite Security Systems) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-18T03:43:28.172Z	Reported to Red Hat.

CNA	2026-03-18T00:00:00.000Z	Made public.

Workarounds

CNA: To mitigate this vulnerability, restrict the outbound network access of the Keycloak instance. Configure firewall rules to prevent the Keycloak server from initiating connections to internal network segments, especially to well-known cloud metadata service IP addresses such as `169.254.169.254`. For example, on Red Hat Enterprise Linux, you can use `firewalld` to add a rich rule: `sudo firewall-cmd --permanent --zone=public --add-rich-rule='rule family="ipv4" destination address="169.254.169.254" reject'` `sudo firewall-cmd --reload` This may impact other services if they legitimately rely on accessing these internal IPs. Additionally, ensure that any configured `sector_identifier_uri` values are thoroughly validated to only point to trusted, external URLs that do not perform redirects to internal resources.

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