Org.keycloak.keycloak-services: improper access control on keycloak server when the account account api feature is disabled

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

Summary

CVE	CVE-2026-7500
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 15:16:23 UTC
Updated	2026-04-30 15:48:26 UTC
Description	When Keycloak is started with `--features-disabled=account,account-api`, the Account REST API is only partially disabled. I

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from secalert@redhat.com

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

Problem Types: CWE-425 | CWE-425 Direct Request ('Forced Browsing')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Keycloak	Not specified	Not specified

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-7500	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 Evan Hendra for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-30T14:31:57.661Z	Reported to Red Hat.
CNA	2026-04-30T00:00:00.000Z	Made public.

Workarounds

CNA: To reduce the attack surface, restrict network access to the Keycloak server's administration and API endpoints to trusted networks or hosts. This limits the ability of unauthorized users to interact with the server and potentially exploit this improper access control vulnerability. If the Keycloak service is reloaded or restarted, ensure that firewall rules or network access controls remain in effect.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report