Org.keycloak.services.resources.account: improper access control leading to mfa deletion and account takeover in keycloak account rest api

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-3429
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-11 17:16:59 UTC
Updated	2026-04-02 14:16:32 UTC
Description	A flaw was identified in the Account REST API of Keycloak that allows a user authenticated at a lower security level to perfo

Risk And Classification

Primary CVSS: v3.1 4.2 MEDIUM from secalert@redhat.com

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

EPSS: 0.000450000 probability, percentile 0.139350000 (date 2026-04-02)

Problem Types: CWE-284 | CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	4.2	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	4.2	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

Availability

None

CVSS:3.1/AV:N/AC:H/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 26.4	unaffected 26.4-14 * rpm	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 26.4.11	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/errata/RHSA-2026:6478	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2026-3429	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2026:6477	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 hamayanhamayan for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-02T09:10:32.484Z	Reported to Red Hat.
CNA	2026-03-02T00:00:00.000Z	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.