Keycloak-services: improper authorization in keycloak organization mapper allows unauthorized organization claims

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

Summary

CVE	CVE-2025-1391
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-02-17 14:15:08 UTC
Updated	2026-05-06 17:16:19 UTC
Description	A flaw was found in the Keycloak organization feature, which allows the incorrect assignment of an organization to a user if

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-284 | CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	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

vailability

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
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0.10-3 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0-11 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.0	unaffected 26.0-12 * rpm	Not specified

References

Reference	Source	Link	Tags
github.com/keycloak/keycloak/pull/37235	secalert@redhat.com	github.com	
access.redhat.com/errata/RHSA-2025:2545	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
github.com/keycloak/keycloak/issues/37169	secalert@redhat.com	github.com	
access.redhat.com/security/cve/CVE-2025-1391	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:2544	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-02-17T07:46:40.184Z	Reported to Red Hat.
CNA	2025-02-17T00:00:00.000Z	Made public.

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**