



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

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2025-1391
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-02-17 14:15:08 UTC
<b>Updated</b>	2026-05-06 17:16:19 UTC
<b>Description</b>	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

Integrity

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
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	<a href="https://github.com">github.com</a>	
access.redhat.com/errata/RHSA-2025:2545	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
github.com/keycloak/keycloak/issues/37169	secalert@redhat.com	<a href="https://github.com">github.com</a>	
access.redhat.com/security/cve/CVE-2025-1391	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
access.redhat.com/errata/RHSA-2025:2544	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)