



# Keycloak: keycloak idor in realm client creating/deleting

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

## Summary

<b>CVE</b>	CVE-2025-14777
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-12-16 05:16:11 UTC
<b>Updated</b>	2026-04-02 14:16:24 UTC
<b>Description</b>	A flaw was found in Keycloak. An IDOR (Broken Access Control) vulnerability exists in the admin API endpoints for authoriz

## Risk And Classification

**Primary CVSS:** v3.1 6 MEDIUM from secalert@redhat.com

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

**Problem Types:** CWE-289 | CWE-289 Authentication Bypass by Alternate Name

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:L
3.1	CNA	CVSS	6	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:L

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**High**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**Low**

Integrity

**High**

Availability

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

## 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

## References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:6478	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>	
access.redhat.com/security/cve/CVE-2025-14777	secalert@redhat.com	<a href="https://access.redhat.com">access.redhat.com</a>	
access.redhat.com/errata/RHSA-2026:6477	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

## Vendor Comments And Credit

## Discovery Credit

**CNA:** Red Hat would like to thank Joshua Rogers for reporting this issue. (en)

## Additional Advisory Data

Source	Time	Event
CNA	2025-12-16T04:55:24.347Z	Reported to Red Hat.
CNA	2025-12-16T04:57:00.000Z	Made public.

## Workarounds

**CNA:** Mitigation for this issue is either not available or the currently available options do not 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.

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**