Keycloak: keycloak idor in realm client creating/deleting

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-14777
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-16 05:16:11 UTC
Updated	2026-04-02 14:16:24 UTC
Description	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

Low

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	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2025-14777	secalert@redhat.com	access.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 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.

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