



Keycloak: org.keycloak.authorization: keycloak: unauthorized resource modification due to improper access control

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

Summary

CVE	CVE-2026-4628
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-23 09:16:26 UTC
Updated	2026-04-01 14:29:05 UTC
Description	A flaw was found in Keycloak. An improper Access Control vulnerability in Keycloak's User-Managed Access (UMA) resource

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from secalert@redhat.com

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

EPSS: 0.000290000 probability, percentile 0.083440000 (date 2026-04-01)

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

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Build Of Keycloak	-	All	All	All

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 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/security/cve/CVE-2026-4628	secalert@redhat.com	access.redhat.com	Vendor Advisory
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Vendor Advisory
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 Evan Hendra for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-23T07:44:56.514Z	Reported to Red Hat.
CNA	2026-03-23T00:00:00.000Z	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](#) 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](#).

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