Keycloak: keycloak: uma policy bypass allows authenticated users to gain unauthorized access to victim-owned resources.

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-4636
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-02 13:16:27 UTC
Updated	2026-04-02 17:16:30 UTC
Description	A flaw was found in Keycloak. An authenticated user with the uma_protection role can bypass User-Managed Access (UMA

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from secalert@redhat.com

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

Problem Types: CWE-551 | CWE-551 Incorrect Behavior Order: Authorization Before Parsing and Canonicalization

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2.15-1 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2-18 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2	unaffected 26.2-18 * rpm	Not specified
CNA	Red Hat	Red Hat Build Of Keycloak 26.2.15	Not specified	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	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/security/cve/CVE-2026-4636	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6478	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6476	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6475	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.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

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2026-03-23T08:15:12.427Z	Reported to Red Hat.
CNA	2026-04-02T12:30:00.000Z	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 registred 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