Keycloak: keycloak: user enumeration via differential error messages

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-4633
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-23 11:16:25 UTC
Updated	2026-04-01 14:26:47 UTC
Description	A flaw was found in Keycloak. A remote attacker can exploit differential error messages during the identity-first login flow wh

Risk And Classification

Primary CVSS: v3.1 3.7 LOW from nvd@nist.gov

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

EPSS: 0.000490000 probability, percentile 0.153070000 (date 2026-04-01)

Problem Types: CWE-209 | CWE-209 Generation of Error Message Containing Sensitive Information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	secalert@redhat.com	Secondary	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Exploit, Issue Tracking, Vendor Advisory
access.redhat.com/security/cve/CVE-2026-4633	secalert@redhat.com	access.redhat.com	Vendor Advisory
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	2026-03-23T08:34:37.879Z	Reported to Red Hat.
CNA	2025-03-23T05:05:00.000Z	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.