



Keycloak-services: keycloak admin rest api: improper access control leads to sensitive role metadata information disclosure

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2025-14082
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-10 09:15:46 UTC
Updated	2026-04-02 14:16:22 UTC
Description	A flaw was found in Keycloak Admin REST (Representational State Transfer) API. This vulnerability allows information disc

Risk And Classification

Primary CVSS: v3.1 2.7 LOW from secalert@redhat.com

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

EPSS: 0.000120000 probability, percentile 0.016050000 (date 2026-04-07)

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

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	2.7	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	2.7	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	High
User Interaction	None
Scope	Unchanged
Confidentiality	

Low

Integrity

None

Availability

None

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

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/security/cve/CVE-2025-14082	secalert@redhat.com	access.redhat.com	
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/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 Muhammad Usman (HackerSSG) (securetackles) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-05T05:12:33.293Z	Reported to Red Hat.
CNA	2025-12-05T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options don't 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](#).

Free CVE JSON API [cve.report/api](#)

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