Ansible-collection-community-general: ansible-collection-community-general: keycloak user module leaks credentials in verbose output

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-14010
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-04 10:16:00 UTC
Updated	2026-05-06 17:16:18 UTC
Description	A flaw was found in ansible-collection-community-general. This vulnerability allows for information exposure (IE) of sensitive

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from secalert@redhat.com

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

Problem Types: CWE-532 | CWE-532 CWE-532 Insertion of Sensitive Information into Log File

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality

High

ntegrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Community.general	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ansible-collections	Ansible Community General Collection	affected 7.1.0 9.5.13 semver	Not specified
CNA	Ansible-collections	Ansible Community General Collection	affected 10.0.0 10.7.6 semver	Not specified
CNA	Ansible-collections	Ansible Community General Collection	affected 11.0.0 11.4.1 semver	Not specified
CNA	Ansible-collections	Ansible Community General Collection	affected 12.0.0 12.2.0 semver	Not specified
CNA	Red Hat	Red Hat Ceph Storage 5	Not specified	Not specified
CNA	Red Hat	Red Hat Ceph Storage 6	Not specified	Not specified
CNA	Red Hat	Red Hat Ceph Storage 7	Not specified	Not specified
CNA	Red Hat	Red Hat Ceph Storage 8	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 17.1	Not specified	Not specified
CNA	Red Hat	Red Hat OpenStack Platform 18.0	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2025-14010	secalert@redhat.com	access.redhat.com	Vendor Adv
github.com/ansible-collections/community.general/issues/11000	secalert@redhat.com	github.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Track
github.com/ansible-community/ansible-build-data/blob/main/12/CHANGELOG-v...	secalert@redhat.com	github.com	
github.com/ansible-collections/community.general/pull/11005	secalert@redhat.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Chris Conway for reporting this issue. (en)

CNA: Red Hat would like to thank Chris Conway for reporting this issue. (cn)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-04T09:28:27.098Z	Reported to Red Hat.
CNA	2025-12-04T00:00:00.000Z	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.