



## Bug 2418774 (CVE-2025-14010) - CVE-2025-14010 ansible-collection-community-general: ansible-collection-community-general: Keycloak user module leaks credentials in verbose output

**Keywords:** Security

**Reported:** 2025-12-04 09:34 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2025-12-04 09:50 UTC ([History](#))

**Alias:** CVE-2025-14010

**CC List:** 18 users ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**


**Whiteboard:**

**Depends On:** [2418776](#) [2418777](#) [2418778](#)  
[2418779](#) [2418780](#)

**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)

**Attachments** ([Terms of Use](#))

OSIDB Bzimport  2025-12-04 09:34:04 UTC[Description](#)

This vulnerability arises from the `community.general.keycloak_user` module exposing the `credentials[].value` field in verbose output. Because this field typically contains plaintext passwords, running Ansible with `-vvv` or similar debug modes inadvertently leaks sensitive credentials. Attackers or unauthorized users with access to logs could retrieve these secrets and potentially compromise Keycloak accounts or administrative access.

---

**Note**

You need to [log in](#) before you can comment on or make changes to this bug.

