CVE-2025-24859: Apache Roller Insufficient Session Expiration on Password Change

Vairav CVE Report

Date: April 16, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A critical session management vulnerability, **CVE-2025-24859**, has been identified in Apache Roller versions prior to 6.1.5. This flaw arises from improper invalidation of active user sessions following password changes. Consequently, attackers with access to compromised sessions can maintain unauthorized access even after credentials are updated. The vulnerability has been assigned a **CVSS v4.0 score of 10.0**, indicating maximum severity.

VULNERABILITY DETAILS

CVE-2025-24859

- **Description:** In Apache Roller versions before 6.1.5, when a user's password is changed—either by the user or an administrator—existing active sessions are not properly invalidated. This oversight allows continued access through old sessions, potentially enabling unauthorized access if credentials were previously compromised. The root cause is the absence of centralized session management to invalidate sessions upon password changes or user deactivation.
- **Impact:** An attacker with access to a user's session can continue to interact with the application even after the user's password has been changed. This undermines standard security practices and poses significant risks, especially in environments where session hijacking is a concern.
- **CVSS v4.0 score:** 10.0 (Critical)

AFFECTED VERSIONS

- Apache Roller versions up to and including 6.1.4

EXPLOIT DETAILS

This vulnerability is particularly concerning in environments where Apache Roller is used as a blogging or content management platform with multiple users. If an attacker gains access to a user's session—through methods like session hijacking—they can maintain access even after the user changes their password. This persistent unauthorized access can lead to data breaches, unauthorized content modifications, and further exploitation of the system.

RECOMMENDED ACTIONS

Patch & Upgrade:

- Upgrade to Apache Roller version 6.1.5

ADDITIONAL SECURITY MEASURES

- Implement centralized session management to ensure all active sessions are invalidated upon password changes or user deactivation.
- Regularly monitor active sessions and provide administrators with tools to forcibly terminate sessions when necessary.
- Educate users about the importance of logging out from sessions, especially on shared or public devices.

REFERENCES

- https://thehackernews.com/2025/04/critical-apache-roller-vulnerability.html
- https://app.opencve.io/cve/CVE-2025-24859

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone:	+977-01-4541540
Mobile:	+977-9820105900
Email:	sales@vairavtech.com
Website:	https://vairavtech.com