مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Apache Roller

Tracking #:432317080

Date:15-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in Apache Roller, a widely used Java-based blogging platform.

TECHNICAL DETAILS:

A critical vulnerability has been discovered in **Apache Roller**, a widely used Java-based blogging platform. Tracked as **CVE-2025-24859** and assigned a **CVSS v4 score of 10 (Critical)**, this flaw concerns **insufficient session expiration following a user password change**. This means that if a user's password is changed—either by themselves or an administrator—**any previously active sessions remain valid**, allowing potential continued unauthorized access.

- **Vulnerability ID**:CVE-2025-24859
- **Severity**: CVSS v4 Score: 10 (Critical)
- **Affected Software**: Apache Roller Versions: 1.0.0 – 6.1.4
- **Unaffected Software**: Apache Roller 6.1.5 and above

A **session management flaw** in Apache Roller before version 6.1.5 allows existing user sessions to **remain active after a password change**. This behavior contradicts standard security expectations, where a password change should invalidate all current sessions to prevent continued access by any unauthorized actor.

Impact:

- An attacker with access to a compromised session token can continue accessing the application even after the user or an administrator changes the account password.
- This undermines incident response actions intended to remove unauthorized access.

Resolution:

- The vulnerability has been **patched in version 6.1.5** by introducing **centralized session management**, ensuring that all active sessions are invalidated on password changes or account disablement.

RECOMMENDATIONS:

1. **Upgrade Immediately:**
   - Update all Apache Roller deployments to fixed version or later.
   - Validate that the upgrade process completes successfully and old versions are fully removed.
2. **Session Monitoring**
   - Audit current user sessions for unusual activity.
   - Log out all user sessions post-upgrade as a precaution.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://lists.apache.org/thread/4j906k16v21kdx8hk87gl7663sw7lg7f