مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in pac4j-jwt

Tracking #:432318538

Date:08-03-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in pac4j-jwt that may allow authentication bypass and unauthorized privilege escalation under certain conditions.

TECHNICAL DETAILS:

A critical vulnerability has been discovered in pac4j-jwt, a widely used Java library for authentication using JSON Web Tokens (JWT). The flaw could allow remote attackers to bypass authentication and forge administrative credentials under certain conditions.

Vulnerability Details

- **CVE ID:** CVE-2026-29000
- **Severity:** Critical (CVSS 10.0)
- The vulnerability exists in the **JwtAuthenticator** component when handling encrypted JWT tokens (JWE). Due to improper validation logic, the library may accept an unsigned token after decryption and skip the signature verification process. This could allow attackers to craft forged tokens containing arbitrary user or administrator claims, potentially leading to authentication bypass.

Affected Versions

- pac4j-jwt
  - Version **4.x**
  - Version **5.x**
  - Version **6.x**

Fixed Versions

- **4.x branch:** 4.5.9 or later
- **5.x branch:** 5.7.9 or later
- **6.x branch:** 6.3.3 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Vendor.

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://nvd.nist.gov/vuln/detail/CVE-2026-29000