An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2603130217

NCSC Advisory

pac4j: pac4j-jwt

CVE-2026-29000

13th, March 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-29000

Published: 2026-03-04

Vendor: pac4j

Product: pac4j-jwt

CVSS Score[1]: 9.3

Products Affected

Product	Version
pac4j-jwt	4.0 < 4.5.9
pac4j-jwt	5.0 < 5.7.9
pac4j-jwt	6.0 < 6.3.3

Impact

pac4j-jwt versions prior to 4.5.9, 5.7.9, and 6.3.3 contain an authentication bypass vulnerability in JwtAuthenticator when processing encrypted JWTs that allows remote attackers to forge authentication tokens. Attackers who possess the server's RSA public key can create a JWE-wrapped PlainJWT with arbitrary subject and role claims, bypassing signature verification to authenticate as any user including administrators.,

Common Weakness Enumeration (CWE)[2]: CWE-347: CWE-347 Improper Verification of Cryptographic Signature

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: Unknown

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from pac4j.

- https://nvd.nist.gov/vuln/detail/CVE-2026-29000
- https://www.cve.org/CVERecord?id=CVE-2026-29000
- https://www.pac4j.org/blog/security-advisory-pac4j-jwt-jwtauthenticator.html
- https://www.codeant.ai/security-research/pac4j-jwt-authentication-bypass-public-key
- https://www.vulncheck.com/advisories/pac4j-jwt-jwtauthenticator-authentication-bypass