ultraviolet

THREAT ADVISORY

Pac4j-JWT Vulnerability

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
March 5, 2026
TLP:GREEN

Executive Snapshot

CVE-2026-29000 is a critical vulnerability in pac4j-jwt which enables a critical JSON Web Token (JWT) authentication bypass in some JSON Web Encryption token (JWE) processing paths, allowing attackers to impersonate arbitrary users by submitting forged tokens that may not undergo proper signature verification. Security leadership should treat this as an urgent identity-layer risk across any service that relies on pac4j for authentication.

- Patch immediately: Upgrade pac4j-jwt to a fixed release on your major line (4.5.9+, 5.7.9+, or 6.3.3+) and prioritize Internet-facing and shared authentication components first.
- Find and scope exposure: Inventory all applications and gateways using pac4j for JWT auth, specifically flagging any endpoints that accept JWEs (encrypted JWTs) and map downstream trust relationships (SSO, APIs, microservices).
- Fail closed on JWT validation: Enforce strict acceptance of signed JWTs (JWS) with an explicit allowlist of algorithms, validate issuer/audience, and disable JWE acceptance where feasible until patches are fully deployed.

TIDE Team Analysis

CVE-2026-29000 is a critical authentication bypass in the pac4j-jwt module's JwtAuthenticator logic that can allow a remote attacker to authenticate as any user (including administrators) by forging a token that the application treats as valid. The risk is amplified in real deployments because the attacker only needs the server's RSA public key, which is often intentionally discoverable in JWT ecosystems (for example via JWKS publication or certificates).

Many pac4j deployments follow a two-layer JWT pattern: JWE encryption (confidentiality) combined with JWS signatures (integrity and authenticity). The vulnerable behavior is triggered in flows that accept encrypted JWTs (JWEs). After decryption, the authenticator can reach a state where it processes the resulting JWT content without correctly enforcing signature verification, allowing attacker-controlled claims to be treated as trusted identity data.

At a code-path level, the bypass stems from how pac4j converts the decrypted token into a "signed JWT" representation for verification. Under certain token constructions, this conversion yields a null signed-JWT object; the implementation gates signature verification behind a conditional check, so verification is skipped when that object is null. Critically, the logic still proceeds to build an authenticated user profile from the unverified claims (e.g., sub, roles, groups), creating an impersonation primitive.

In practice, exploitation is straightforward in affected configurations: the attacker obtains the target's RSA public key, crafts a JWE token encrypted to that key, and embeds an inner token payload containing attacker-chosen identity and authorization claims. Because the failure is in authentication logic—not cryptography—the attacker does not need credentials or the private key; they only need to craft a token that exercises the vulnerable parsing/verification branch.

The impact is full account compromise within any system that relies on pac4j-derived JWT claims to establish authentication and authorization context. The most severe outcomes include administrator impersonation, privilege escalation, and onward access to downstream services that trust the same identity assertions. This can become an enterprise-wide problem if a shared identity provider, gateway, or common auth library version is reused across multiple internal applications.

Why It Matters

This matters because CVE-2026-29000 sits in the identity/authentication layer, which is the same “blast radius” characteristic that made Log4Shell (Log4j) and other ecosystem-wide flaws so disruptive: a widely embedded component, used transitively across many products, that turns into a remote, pre-auth compromise primitive when exposed. In practical terms, an authentication bypass in a common library can be just as operationally catastrophic as an RCE—because once an attacker can mint “valid” sessions as any user, they can pivot into admin consoles, management APIs, CI/CD systems, and downstream services that trust the same identity assertions. The risk compounds in modern architectures where gateways and shared auth middleware provide a single choke point: one vulnerable implementation can translate into fleet-wide exposure.

Patching urgency is higher than the average “critical CVE” because public exploit material is already available, including a working proof-of-concept demonstrating impersonation via a crafted JWE-wrapped token that bypasses signature verification. Once a PoC exists, exploitation rapidly shifts from “theoretical” to “automatable,” and the window between disclosure and opportunistic scanning typically compresses to days. Treat this like a Log4j-class response motion: patch now (fixed lines: 4.5.9+, 5.7.9+, 6.3.3+), aggressively inventory where pac4j JWT auth is used (especially JWE acceptance), and apply compensating controls only as a short-lived bridge—not as a substitute for upgrading.

How to Respond

- Strictly adhere to CyberSecurity Fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Ensure all pac4j libraries are upgraded to the appropriate version which patches this vulnerability (4.5.9+, 5.7.9+, or 6.3.3+).
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a RedTeam or PurpleTeam engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Monitoring and analyzing new vulnerabilities, public POC code, and community sentiment.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---