مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Jenkins Plugins

Tracking #:432317272

Date:15-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Jenkins has released a critical security advisory disclosing multiple vulnerabilities across several widely-used plugins.

TECHNICAL DETAILS:

Jenkins has released a critical security advisory disclosing multiple vulnerabilities across several widely-used plugins. Two vulnerabilities are rated Critical, posing immediate risk to the integrity and security of Jenkins environments. These issues range from authentication bypass, stored XSS, and CSRF, to SSL/TLS validation disabling, and improper claim validation.

1. OpenID Connect Provider Plugin - Improper Claim Validation

- **CVE**: CVE-2025-47884
- **Severity**: Critical
- **Affected Versions**: ≤ 96.vee8ed882ec4d
- **Fixed In**: 111.v29fd614b_3617
- **Description**:
  The plugin improperly relies on potentially attacker-controlled environment variables (e.g., JOB_URL) in the claim templates for build ID tokens. If used with plugins like *Environment Injector*, attackers can forge ID tokens to impersonate trusted jobs—resulting in unauthorized access to external systems.

2. Health Advisor by CloudBees Plugin - Stored XSS

- **CVE**: CVE-2025-47885
- **Severity**: High
- **Affected Versions**: ≤ 374.v194b_d4f0c8c8
- **Fixed In**: 374.376.v3a_41a_a_142efe
- **Description**:
  Server responses from the Jenkins Health Advisor were not properly escaped, enabling stored Cross-Site Scripting (XSS) attacks. An attacker controlling server responses could inject malicious scripts, affecting Jenkins users who view plugin-related pages.

3. Cadence vManager Plugin - CSRF & Missing Permission Checks

- **CVE**: CVE-2025-47886 (CSRF), CVE-2025-47887 (Permission Bypass)
- **Severity**: Medium
- **Affected Versions**: ≤ 4.0.1-286.v9e25a_740b_a_48
- **Fixed In**: 4.0.1-288.v8804b_ea_a_cb_7f
- **Description**:
  Lack of permission checks and POST validation on form inputs allowed:
  - **CSRF attacks** exploiting GET requests.
  - Unauthorized connections to attacker-specified URLs using credentials injected by the attacker.

4. DingTalk Plugin - SSL/TLS Validation Disabled

- **CVE**: CVE-2025-47888
- **Severity**: Medium
- **Affected Versions**: ≤ 2.7.3

- **Fix Available**:No
- **Description**:
  Plugin disables certificate and hostname validation on all connections to configured DingTalk webhooks. This exposes Jenkins to **MITM (Man-in-the-Middle)** and **data interception** risks.

5. WSO2 Oauth Plugin - Authentication Bypass

- **CVE**: CVE-2025-47889
- **Severity**: Critical
- **Affected Versions**: ≤ 1.0
- **Fix Available**: No
- **Description**:
  The plugin accepts any username and password without validating authentication claims. Attackers can log in with **any credential**, even nonexistent usernames. In insecure authorization strategies (e.g., "Logged-in users can do anything"), this may grant **admin access**.

RECOMMENDATIONS:

- Immediately update all plugins where patches are available.
- Disable or uninstall vulnerable plugins with no fix.

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://www.jenkins.io/security/advisory/2025-05-14/