مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in Jenkins plugins

Tracking #:432317881

Date:30-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple vulnerabilities across various Jenkins plugins, including high-severity replay, command injection, and XML External Entity (XXE) flaws. These issues may allow attackers to gain unauthorized access, execute arbitrary code, or expose sensitive data.

TECHNICAL DETAILS:

High-Severity Vulnerabilities

- CVE-2025-64131 — Replay Vulnerability in SAML Plugin
- CVE-2025-64134 — XXE Vulnerability in JDepend Plugin
- CVE-2025-64140 — Shell Command Injection in Azure-CLI Plugin

Impact:

These vulnerabilities could allow attackers to gain unauthorized access to Jenkins instances, execute arbitrary commands on the Jenkins controller, or exfiltrate sensitive data through XML external entity (XXE) attacks. Exploitation may result in full compromise of the Jenkins environment and underlying system.

Medium Severity Vulnerabilities

- CVE-2025-64132 — Missing Permission Checks in MCP Server Plugin
- CVE-2025-64133 — CSRF Vulnerability in Extensible Choice Parameter Plugin
- CVE-2025-64135 — Java Protection Mechanism Disabled in Eggplant Runner Plugin
- CVE-2025-64136 / CVE-2025-64137 — CSRF Vulnerability and Missing Permission Check in Themis Plugin
- CVE-2025-64138 / CVE-2025-64139 — CSRF Vulnerability and Missing Permission Check in Start Windocks Containers Plugin
- CVE-2025-64141 / CVE-2025-64142 — CSRF Vulnerability and Missing Permission Checks in Nexus Task Runner Plugin
- CVE-2025-64143 — Authorization Token Stored in Plain Text by OpenShift Pipeline Plugin
- CVE-2025-64144 / CVE-2025-64145 — API Tokens Stored in Plain Text by ByteGuard Build Actions Plugin
- CVE-2025-64146 / CVE-2025-64147 — API Keys Stored in Plain Text by Curseforge Publisher Plugin
- CVE-2025-64148 — Missing Permission Check in Publish to Bitbucket Plugin
- CVE-2025-64149 / CVE-2025-64150 — CSRF Vulnerability and Missing Permission Check in Publish to Bitbucket Plugin

Impact:

These vulnerabilities can expose sensitive credentials, allow unauthorized access or configuration changes, and enable cross-site request forgery (CSRF) attacks. Exploitation may lead to data leakage, unauthorized builds, or external connections initiated from Jenkins, weakening overall security posture.

Affected Versions

- **azure-cli Plugin** up to and including 0.9
- **ByteGuard Build Actions Plugin** up to and including 1.0
- **Curseforge Publisher Plugin** up to and including 1.0
- **Eggplant Runner Plugin** up to and including 0.0.1.301.v963cffe8ddb_8
- **Extensible Choice Parameter Plugin** up to and including 239.v5f5c278708cf

- **JDepend Plugin** up to and including 1.3.1
- **MCP Server Plugin** up to and including 0.84.v50ca_24ef83f2
- **Nexus Task Runner Plugin** up to and including 0.9.2
- **OpenShift Pipeline Plugin** up to and including 1.0.57
- **Publish to Bitbucket Plugin** up to and including 0.4
- **SAML Plugin** up to and including 4.583.vc68232f7018a_
- **Start Windocks Containers Plugin** up to and including 1.4
- **Themis Plugin** up to and including 1.4.1

Fixed Versions

- **MCP Server Plugin** should be updated to version 0.86.v7d3355e6a_a_18
- **SAML Plugin** should be updated to version 4.583.585.v22ccc1139f55

Currently, no fixes are available for the following plugins:

- azure-cli Plugin
- ByteGuard Build Actions Plugin
- Curseforge Publisher Plugin
- Eggplant Runner Plugin
- Extensible Choice Parameter Plugin
- JDepend Plugin
- Nexus Task Runner Plugin
- OpenShift Pipeline Plugin
- Publish to Bitbucket Plugin
- Start Windocks Containers Plugin
- Themis Plugin

RECOMMENDATIONS:

- **Immediate Action:** Update SAML and MCP Server plugins to the fixed versions
- **Mitigation:** Restrict access to Jenkins instances, limit permissions, and monitor for replay or CSRF attempts.
- **Unpatched Plugins:** Consider disabling or sandboxing unmaintained plugins until patches are released.

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/2025-10-29/