مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Jenkins

Tracking #:432317028

Date:03-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Jenkins released a security advisory detailing multiple vulnerability affecting its core and several plugins.

TECHNICAL DETAILS:

Jenkins released a security advisory detailing multiple vulnerabilities affecting its core and several plugins. These vulnerabilities range from improper permission checks to insecure storage of secrets and API keys, exposing sensitive data and enabling potential exploitation by attackers. The most severe vulnerability, affecting the Templating Engine Plugin, allows arbitrary code execution due to a sandbox bypass. Administrators are strongly encouraged to update affected Jenkins versions and plugins to mitigate risks. For some plugins, no fixes are currently available, requiring alternative security measures

Detailed Vulnerability Breakdown

1. Missing Permission Check - Agent Configuration (CVE-2025-31720, CVE-2025-31721)
   - Severity: Medium (CVSS Score: 5.5 - 6.3)
   - Affected Versions: Jenkins 2.503 and earlier, LTS 2.492.2 and earlier
   - Impact: Attackers with Computer/Create permission but without Computer/Extended Read or Computer/Configure permissions can copy agent configurations, gaining access to encrypted secrets.
   - Fix: Jenkins 2.504 and LTS 2.492.3 require appropriate permissions to copy agents.

2. Sandbox Bypass in Templating Engine Plugin (CVE-2025-31722)
   - Severity: High (CVSS Score: 8.8)
   - Affected Versions: Templating Engine Plugin 2.5.3 and earlier
   - Impact: Attackers with Item/Configure permission can execute arbitrary code on the Jenkins controller by exploiting folder-scoped libraries.
   - Fix: Update to Templating Engine Plugin 2.5.4, which enforces script sandboxing.

3. CSRF Vulnerability in Simple Queue Plugin (CVE-2025-31723)
   - Severity: Medium (CVSS Score: 6.1)
   - Affected Versions: Simple Queue Plugin 1.4.6 and earlier
   - Impact: Attackers can manipulate the build queue order via CSRF.
   - Fix: Update to Simple Queue Plugin 1.4.7, which requires POST requests for sensitive actions.

4. API Keys and Credentials Stored in Plaintext (Multiple CVEs)
   - Severity: Medium
   - Affected Plugins:
     - Cadence vManager Plugin (CVE-2025-31724) - Fixed in version 4.0.1-286.v9e25a_740b_a_48.
     - monitor-remote-job Plugin (CVE-2025-31725) - No fix available.
     - Stack Hammer Plugin (CVE-2025-31726) - No fix available.
     - AsakusaSatellite Plugin (CVE-2025-31727 & CVE-2025-31728) - No fix available.
   - Impact: Unencrypted API keys and passwords can be accessed by users with Item/Extended Read permission or direct access to the Jenkins controller filesystem.

- Fix:
  - Update affected plugins where possible.
  - Rotate API keys and passwords stored in job configurations.
  - Consider removing or disabling plugins without fixes.

RECOMMENDATIONS:

- Update Jenkins Core & Affected Plugins to the fixed version.

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/2025-04-02/