مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Jenkins Plugins

Tracking #:432316780

Date:23-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a series of vulnerabilities have been identified in several Jenkins plugins, posing various security risks ranging from unauthorized credential access to potential privilege escalation.

TECHNICAL DETAILS:

A series of vulnerabilities have been identified in several Jenkins plugins, posing various security risks ranging from unauthorized credential access to potential privilege escalation.

Vulnerabilities Overview:
The following vulnerabilities have been identified:

1. **GitLab Plugin - Incorrect Permission Check (CVE-2025-24397):**
   - **Severity:** Medium
   - **Description:** The GitLab Plugin does not properly check permissions when accessing certain HTTP endpoints, allowing attackers with global Item/Configure permissions to enumerate credential IDs of GitLab API tokens and other sensitive credentials.
2. **Bitbucket Server Integration Plugin - CSRF Bypass (CVE-2025-24398):**
   - **Severity:** High
   - **Description:** A permissive implementation of CSRF protection in versions 2.1.0 to 4.1.3 enables attackers to bypass CSRF protection for any URL, leading to potential attacks.
3. **OpenId Connect Authentication Plugin - Case Sensitivity Vulnerability (CVE-2025-24399):**
   - **Severity:** High
   - **Description:** The plugin treats usernames as case-insensitive, allowing attackers to impersonate users by providing usernames with different letter cases, which could potentially lead to administrator access.
4. **Zoom Plugin - Plain Text Token Storage (CVE-2025-0142):**
   - **Severity:** Medium
   - **Description:** Zoom tokens are stored in job config.xml files without encryption, allowing unauthorized users to view these tokens if they have Item/Extended Read permissions or file system access.
5. **Zoom Plugin - Token Exposure (CVE Pending):**
   - **Severity:** Low
   - **Description:** In versions 1.5 and earlier, the Zoom Plugin does not mask integration tokens displayed in the job configuration form, increasing the risk of token exposure.
6. **Eiffel Broadcaster Plugin - Cache Confusion (CVE-2025-24400):**
   - **Severity:** Medium
   - **Description:** The plugin uses a credential ID as a cache key, allowing attackers to potentially replace a legitimate credential with their own, impacting the integrity of signed events sent to RabbitMQ.
7. **Folder-based Authorization Strategy Plugin - Permission Granting Flaw (CVE-2025-24401):**
   - **Severity:** Medium

- **Description:** The plugin fails to verify that permissions granted are enabled, potentially allowing unauthorized users to access functionality they should not have permission to use.

8. **Azure Service Fabric Plugin - CSRF and Permission Check Vulnerabilities (CVE-2025-24402, CVE-2025-24403):**
   - **Severity:** Medium
   - **Description:** The plugin lacks proper permission checks and is susceptible to CSRF attacks on several HTTP endpoints, allowing attackers to potentially manipulate service configurations and expose credentials.

Affected Versions:

- Azure Service Fabric Plugin: Up to version 1.6
- Bitbucket Server Integration Plugin: Up to version 4.1.3
- Eiffel Broadcaster Plugin: Up to version 2.10.2
- Folder-based Authorization Strategy Plugin: Up to version 217.vd5b_18537403e
- GitLab Plugin: Up to version 1.9.6
- OpenId Connect Authentication Plugin: Up to version 4.452.v2849b_d3945fa_
- Zoom Plugin: Up to versions 1.3 and 1.5

Fix Versions:

- Bitbucket Server Integration Plugin: Update to version 4.1.4.
- Eiffel Broadcaster Plugin: Update to version 2.10.3.
- GitLab Plugin: Update to version 1.9.7.
- OpenId Connect Authentication Plugin: Update to version 4.453.v4d7765c854f4.
- Zoom Plugin: Update to version 1.4 and 1.6.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends users to update affected plugins to their latest versions at the earliest.

For plugins without fixes, users should monitor for updates and consider implementing workarounds or additional security measures

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/2025-01-22/