مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Jenkins Security Updates

Tracking #:432316359

Date:03-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

On October 2, 2024, Jenkins released a security advisory detailing multiple vulnerability affecting its core system and several plugins. These vulnerabilities could potentially expose sensitive information or allow unauthorized actions within Jenkins environments.

Vulnerabilities Overview:

1. **Exposure of Multi-line Secrets through Error Messages**
   - **CVE:** CVE-2024-47803
   - **Severity:** Medium
   - **Affected Versions:** Jenkins 2.478 and earlier, LTS 2.462.2 and earlier
   - **Description:** The secretTextarea form field does not redact multi-line secret values in error messages, leading to potential exposure in logs.
   - **Fix:** Update to Jenkins 2.479 or LTS 2.462.3.
2. **Item Creation Restriction Bypass**
   - **CVE:** CVE-2024-47804
   - **Severity:** Medium
   - **Affected Versions:** Jenkins 2.478 and earlier, LTS 2.462.2 and earlier
   - **Description:** Attackers can bypass item creation restrictions via the CLI or REST API, allowing them to create temporary items even when prohibited by authorization strategies.
   - **Fix:** Update to Jenkins 2.479 or LTS 2.462.3.
3. **Revealing Encrypted Credential Values**
   - **CVE:** CVE-2024-47805
   - **Severity:** Medium
   - **Affected Versions:** Credentials Plugin 1380.va_435002fa_924 and earlier (except 1371.1373.v4eb_fa_b_7161e9)
   - **Description:** The plugin fails to redact encrypted values of credentials accessed via REST API or CLI, allowing unauthorized users to view sensitive information.
   - **Fix:** Update to Credentials Plugin version 1381.v2c3a_12074da_b_.
4. **Lack of Audience Claim Validation in OpenId Connect Authentication Plugin**
   - **CVE:** CVE-2024-47806
   - **Severity:** High
   - **Affected Versions:** OpenId Connect Authentication Plugin 4.354.v321ce67a_1de8 and earlier
   - **Description:** This vulnerability allows attackers to potentially gain administrator access by subverting the authentication flow due to missing audience claim validation in ID tokens.
   - **Fix:** Update to OpenId Connect Authentication Plugin version 4.355.v3a_fb_fca_b_96d4.
5. **Lack of Issuer Claim Validation in OpenId Connect Authentication Plugin**
   - **CVE:** CVE-2024-47807
   - **Severity:** High

- **Affected Versions:** OpenId Connect Authentication Plugin 4.354.v321ce67a_1de8 and earlier
- **Description:** Similar to the previous issue, this vulnerability may allow unauthorized access due to missing issuer claim validation in ID tokens during authentication flows.
- **Fix:** Update to OpenId Connect Authentication Plugin version 4.355.v3a_fb_fca_b_96d4.

Affected Versions:

- Jenkins weekly up to and including 2.478
- Jenkins LTS up to and including 2.462.2
- Credentials Plugin up to and including 1380.va_435002fa_924
- OpenId Connect Authentication Plugin up to and including 4.354.v321ce67a_1de8

Fixed Versions:

- Jenkins weekly version 2.479
- Jenkins LTS version 2.462.3
- Credentials Plugin version 1381.v2c3a_12074da_b_
- OpenId Connect Authentication Plugin version 4.355.v3a_fb_fca_b_96d4

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the affected products version 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/2024-10-02/