مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Jenkins Security Updates

Tracking #:432316515

Date:15-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Jenkins has released a security advisory addressing multiple vulnerabilities in several Jenkins plugins.

TECHNICAL DETAILS:

Jenkins, a widely used automation server, has released a critical security advisory addressing multiple vulnerabilities in several Jenkins plugins. These vulnerabilities, identified in high-impact plugins such as **Script Security**, **Pipeline: Groovy**, **Pipeline: Declarative**, **Authorize Project**, **OpenId Connect Authentication**, **IvyTrigger**, and **Shared Library Version Override**, can potentially lead to unauthorized access, code execution, session fixation, stored cross-site scripting (XSS), and sensitive data exposure. These flaws could allow attackers to bypass security controls, escalate privileges, or execute malicious scripts, posing significant risks to the integrity of Jenkins instances.

Vulnerabilities Overview:

1. Missing Permission Check in Script Security Plugin
   - CVE-2024-52549 Severity: Medium
2. Rebuilding a Run with Revoked Script Approval in Pipeline: Groovy Plugin
   - CVE-2024-52550 Severity: High
3. Restarting a Run with Revoked Script Approval in Pipeline: Declarative Plugin
   - CVE-2024-52551Severity: High
4. Stored XSS Vulnerability in Authorize Project Plugin
   - CVE-2024-52552 Severity: High
5. Session Fixation Vulnerability in OpenId Connect Authentication Plugin
   - CVE-2024-52553 Severity: High
6. XXE Vulnerability in IvyTrigger Plugin
   - CVE-2022-46751 Severity: High
7. Script Security Bypass in Shared Library Version Override Plugin
   - CVE-2024-52554 Severity: High

Affected Versions and Fixes:

Plugin	Affected Version(s)	Fixed Version
Authorize Project Plugin	1.7.2 and earlier	1.8.0
IvyTrigger Plugin	1.01 and earlier	1.02
OpenId Connect Authentication Plugin	4.418.vccc7061f5b_6d and earlier	4.421.v5422614eb_e0a_
Pipeline: Declarative Plugin	2.2214.vb_b_34b_2ea_9b_83 and earlier	2.2218.v56d0cda_37c72
Pipeline: Groovy Plugin	3990.vd281dd77a_388 and earlier	3993.v3e20a_37282f8
Script Security Plugin	1367.vdf2fc45f229c and earlier	1368.vb_b_402e3547e7
Shared Library Version Override Plugin	17.v786074c9fce7 and earlier	19.v3a_c975738d4a_

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update all affected plugins to the fixed versions at the earliest.

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/2024-11-13/