Security Advisory 2023-017

Severe Vulnerabilities in Jenkins Products

March 09, 2023 — v1.0

TLP:CLEAR

History:

- *09/03/2023 — v1.0 – Initial publication*

Summary

On March 8, 2023, Jenkins released advisories regarding 2 severe security vulnerabilities in Jenkins server and Update Center [1]. These vulnerabilities are identified by `CVE-2023-27898` and `CVE-2023-27905` and could allow an unauthenticated attacker to execute arbitrary code on the victim's Jenkins server, potentially leading to a complete compromise of the Jenkins server.

Furthermore, these vulnerabilities could be exploited even if the Jenkins server is not directly reachable by attackers and could also impact self-hosted Jenkins servers [2].

Technical Details

The issue is a result of a flaw in the Jenkins' processing of available plugins from the Update Center, thereby potentially enabling a threat actor to upload a plugin with a malicious payload and trigger a cross-site scripting (XSS) attack. Once the victim opens the 'Available Plugin Manager' on their Jenkins server, the XSS is triggered, allowing attackers to run arbitrary code on the Jenkins Server utilising the Script Console API [2].

Since it's also a case of stored XSS wherein the JavaScript code is injected into the server, the vulnerability can be activated without having to install the plugin or even visit the URL to the plugin in the first place.

Affected Products

- Jenkins weekly up to and including 2.393;
- Jenkins LTS up to and including 2.375.3;
- update-center2 up to and including 3.14.

Recommendations

CERT-EU recommends updating Jenkins servers to the latest available version:

- Jenkins weekly should be updated to version 2.394;
- Jenkins LTS should be updated to version 2.375.4 or 2.387.1;
- update-center2 should be updated to version 3.15.

References

[1] https://www.jenkins.io/security/advisory/2023-03-08/

[2] https://blog.aquasec.com/jenkins-server-vulnerabilities