CERT-EU

Security Advisory 2024-014

Critical Remote Code Execution Vulnerability in Jenkins

January 30, 2024 — v1.1

TLP:CLEAR

History:

- *29/01/2024 — v1.0 – Initial publication*
- *30/01/2024 — v1.1 – Fix versions in affected products*

Summary

On January 24, 2024, Jenkins issued fixes for several vulnerabilities, including **CVE-2024-23897**, a critical vulnerability that could allow an attacker to achieve remote code execution. The advisory published provides detailed information on various attack scenarios, exploitation pathways, descriptions of the fixes, and potential workarounds for those unable to immediately apply the security updates.

Multiple proof-of-concept (PoC) exploits for **CVE-2024-23897** are now available [2].

Technical Details

The vulnerability **CVE-2024-23897**, with a CVSS score of 9.8, could allow an unauthenticated attacker with `overall/read` permission to read data from arbitrary files on the Jenkins server [2].

The vulnerability **CVE-2024-23898**, with a CVSS score of 8,8, is a cross-site WebSocket hijacking issue where attackers could execute arbitrary CLI commands by tricking a user into clicking a malicious link [2].

The exploitation of these vulnerabilities could lead to admin privilege escalation and arbitrary remote code execution under certain conditions [1].

Affected Products

- Jenkins weekly up to and including 2.441
- Jenkins LTS up to and including 2.426.2

Recommendations

CERT-EU recommends immediate update of affected Jenkins versions to the latest patched versions.

References

[1] https://www.jenkins.io/security/advisory/2024-01-24/index.html#SECURITY-3314

[2] https://www.bleepingcomputer.com/news/security/exploits-released-for-critical-jenkins-rce-flaw-patch-now/