CYBER ADVISORY

TLP:CLEAR

01 February 2024

Jenkins CI/CD Tool Vulnerability

CVE-2024-23897 | Jenkins | Critical Vulnerability | Active Exploitation

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of a critical vulnerability under active exploitation known as CVE-2024-23897. The vulnerability affects Jenkins 2.441 and earlier versions. The vulnerability additionally affects Jenkins LTS 2.426.2 and earlier versions. The issue lies in the command parser (the args4j library) which has a feature where an '@' character followed by a file path in an argument is replaced with the file's content. r.[1] The vulnerability could be exploited to read the content of binary files that contain cryptographic keys which, under certain conditions, opens the door for several remote code execution (RCE) scenarios and allows attackers to decrypt stored secrets, delete items in Jenkins, and download a Java heap dump of the Jenkins controller process.[2,3]

The Cal-CSIC recommends immediately applying the mitigation methods presented in the Jenkins Security Advisory.

For further information on implementing mitigation, please refer to Jenkins Security Advisory.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of

	cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Security Week; "Critical Jenkins Vulnerability Leads to Remote Code Execution;" https://www.securityweek.com/critical-jenkins-vulnerability-leads-to-remote-code-execution/; accessed 01 February 2024

[2] Splunk; "Security Insights: Jenkins CVE-2024-23897 RCE;" https://www.splunk.com/en_us/blog/security/security-insights-jenkins-cve-2024-23897-rce.html; accessed 01 February 2024

[3] Security Boulevard; "CVE-2024-23897: Assessing the Impact of the Jenkins Arbitrary File Leak Vulnerability;" https://securityboulevard.com/2024/01/cve-2024-23897-assessing-the-impact-of-the-jenkins-arbitrary-file-leak-vulnerability/; accessed 01 February 2024