Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Remote Code Execution Flaws Uncovered in Jenkins

Date of Publication

January 31, 2024

Admiralty Code

A1

TA Number

TA2024040

Summary

Vulnerability Discovered: January 24, 2024
Affected Products: Jenkins, Jenkins LTS, Jenkins Plugins (Git server, Qualys Policy Compliance, Red Hat Dependency Analytics, Log Command)
Impact: Multiple vulnerabilities have been discovered in Jenkins and number of associated plugins, allowing attackers unauthorized data access and execute arbitrary commands. The critical vulnerability CVE-2024-23897, allows attackers to read system files and opens number of attack vectors associated with Remote Code Execution.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-23897 (Critical)	Jenkins Arbitrary File Read Vulnerability	Jenkins, Jenkins LTS	✗	✓	✓
CVE-2024-23898 (High)	Jenkins Cross-site WebSocket Hijacking Vulnerability	Jenkins, Jenkins LTS	✗	✓	✓
CVE-2024-23899 (High)	Jenkins Git Server File Read Vulnerability	Jenkins Git server Plugin	✗	✓	✓
CVE-2023-6148 (High)	Jenkins Qualys Policy Compliance Stored XSS Vulnerability	Jenkins Qualys Policy Compliance	✗	✗	✓
CVE-2023-6147 (High)	Jenkins Qualys Policy Compliance XXE Vulnerability	Jenkins Qualys Policy Compliance	✗	✗	✓
CVE-2024-23905 (High)	Jenkins Red Hat Dependency Analytics Plugin Vulnerability	Jenkins Red Hat Dependency Analytics Plugin	✗	✓	✓
CVE-2024-23904 (High)	Jenkins Log Command File Read Vulnerability	Jenkins Log Command Plugin	✗	✓	✗

Vulnerability Details

#1 Jenkins, an open-source automation server widely employed for Continuous Integration (CI) and Continuous Deployment (CD) in software development, faces significant security risks due to vulnerabilities CVE-2024-23897 and CVE-2024-23898. These vulnerabilities could potentially result in remote code execution if exploited successfully. Notably, several proof-of-concept (PoC) exploits targeting CVE-2024-23897 have been publicly disclosed.

#2 A critical flaw, CVE-2024-23897, arises from the application's CLI command parser, which does not disable a feature that replaces an "@" character followed by a file path in an argument with the file's contents. Consequently, remote attackers can exploit this vulnerability to gain unauthorized access to restricted functionality and potentially execute arbitrary code on the Jenkins controller file system.

#3 This vulnerability allows unauthenticated attackers to read system files, even binary files containing cryptographic keys, under certain preconditions. Once the binary secrets are extracted, it creates a myriad of code execution attack vectors including RCE via Resource Root URLs, "Remember me" cookie, stored XSS attacks and CSRF protection bypass. In addition, the vulnerability also enables attackers to decrypt secrets stored in Jenkins, delete items and download a Java heap dump.

#4 Another high severity flaw CVE-2024-23898 enables a remote attacker to gain unauthorized access to functionality that is typically restricted. This vulnerability stems from the application's lack of validation for the origin of requests sent via the CLI WebSocket endpoint, constituting a cross-site WebSocket hijacking (CSWSH) issue. Consequently, the Jenkins controller may be susceptible to CLI commands issued by a remote attacker.

#5 Jenkins has also identified and addressed other high-severity vulnerabilities impacting several plugins, including the Git server Plugin, Qualys Policy Compliance Scanning Connector Plugin, Red Hat Dependency Analytics Plugin, and Log Command Plugin. The fix for Log Command Plugin vulnerability is not yet available. The impact from these vulnerabilities spanned from information disclosure to remote code execution, underscoring the urgent need for comprehensive security measures and prompt remediation to mitigate the risks posed by these vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-23897	Jenkins: 2.204.2 - 2.441 Jenkins LTS: 2.222.1 - 2.426.2	cpe:2.3:a:jenkins:jenkinsLTS:*:*:*:*:*:*:*:*	CWE-284
CVE-2024-23898	Jenkins: 2.204.2 - 2.441 Jenkins LTS: 2.222.1 - 2.426.2	cpe:2.3:a:jenkins:jenkinsLTS:*:*:*:*:*:*:*:*	CWE-1385
CVE-2024-23899	Git server version 99.va_0826a_b_cdfa_d	cpe:2.3:a:jenkins:Gitserver:*:*:*:*:*:*:*:*	CWE-284
CVE-2023-6148	Qualys Policy Compliance Scanning Connector version 1.0.5 and prior versions	cpe:2.3:a:jenkins:Qualys_Policy_Compliance_Scanning_Connector:*:*:*:*:*:*:*:*	CWE-79
CVE-2023-6147	Qualys Policy Compliance Scanning Connector version 1.0.5 and prior versions	cpe:2.3:a:jenkins:Qualys_Policy_Compliance_Scanning_Connector:*:*:*:*:*:*:*:*	CWE-611
CVE-2024-23905	Red Hat Dependency Analytics version 0.7.1 and prior versions	cpe:2.3:a:jenkins:RedHat_Dependency_Analytics:*:*:*:*:*:*:*:*	CWE-284
CVE-2024-23904	Log Command versions 1.0.2 and prior versions	cpe:2.3:a:jenkins:Log_Command:*:*:*:*:*:*:*:*	CWE-200

Recommendations

Update: It's crucial to update and upgrade to Jenkins version 2.442 or LTS 2.426.3 immediately to mitigate the vulnerabilities. These updates include patches to address the security flaws and enhance the overall security posture of your Jenkins deployment.

Disable CLI access: Disabling access to the Jenkins CLI is a recommended workaround to mitigate the vulnerabilities, especially for administrators who are unable to immediately update to the latest Jenkins versions. By disabling CLI access, you can prevent potential exploitation of these vulnerabilities.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1059 Command and Scripting Interpreter
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	

Patch Details

Update to Jenkins 2.442, LTS 2.426.3
Update to Git server Plugin 99.101.v720e86326c09
Update to Qualys Policy Compliance Scanning Connector Plugin 1.0.6
Update to Red Hat Dependency Analytics Plugin 0.9.0

Link:
https://www.jenkins.io/download/

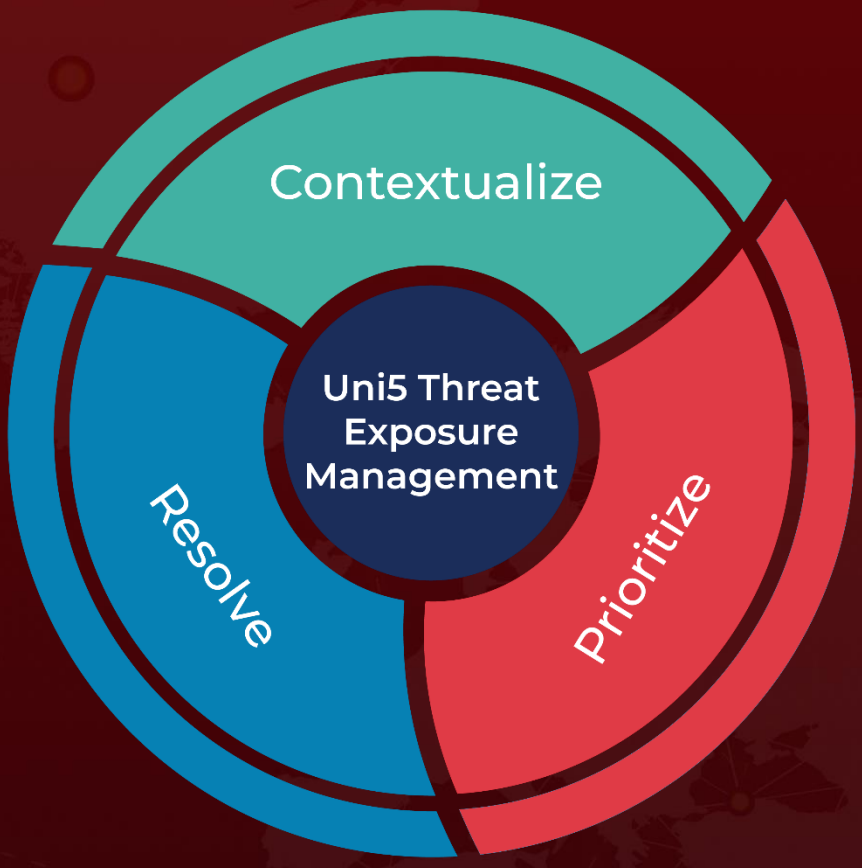
References

https://www.jenkins.io/security/advisory/2024-01-24/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 31, 2024 • 5:50 AM

More at www.hivepro.com