

CVE-2024-23897

Jenkins Command Line Interface (CLI) Path Traversal Vulnerability

Exigent CISA KEV since Aug 19, 2024 Actively exploited Ransomware use known Public exploit module (Metasploit)

Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.

EVRS 94/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.99th percentile · FIRST	CISA DEADLINE Sep 9, 2024 KEV since 2024 · listed over a year
--	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
jenkins	< 2.426.3 < 2.442	2.426.3 · 2.442	NVD

Sources

Vendor guidance	jenkins.io/security/advisory/2024-01-24/#SECURITY-3314	Additional guidance	vicarius.io/vsociety/posts/the-anatomy-of-a-jenkins-vulnerability-cve-2024-23897-revealed-1
NVD	nvd.nist.gov/vuln/detail/CVE-2024-23897	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-0270	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-23897

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.