

CVE-2019-1003030

Jenkins Matrix Project Plugin Remote Code Execution Vulnerability

Exigent CISA KEV since Mar 25, 2022 Actively exploited

A sandbox bypass vulnerability exists in Jenkins Pipeline: Groovy Plugin 2.63 and earlier in pom.xml, src/main/java/org/jenkinsci/plugins/workflow/cps/CpsGroovyShell.java that allows attackers able to control pipeline scripts to execute arbitrary code on the Jenkins master JVM.

EVRS 86 /100 Immediate priority	CVSS V3.1 9.9 Critical · NVD	EPSS 0.971 99.89th percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.971 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.9	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified
CISA required action: Apply updates per vendor instructions.
 Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
pipeline\	groovy ≤ 2.63	after 2.63	NVD
openshift container platform	3.11	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-r6mc-mrvr-23cr	Additional guidance	access.redhat.com/errata/RHSA-2019:0739
NVD	nvd.nist.gov/vuln/detail/CVE-2019-1003030	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-5117	Current data	evulnable.com/vulnerability-management/cve/CVE-2019-1003030

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