

CVE-2017-1000353

Jenkins Remote Code Execution Vulnerability

Exigent

CISA KEV since Oct 2, 2025

Actively exploited

Public exploit module (Metasploit)

Jenkins versions 2.56 and earlier as well as 2.46.1 LTS and earlier are vulnerable to an unauthenticated remote code execution. An unauthenticated remote code execution vulnerability allowed attackers to transfer a serialized Java `SignedObject` object to the Jenkins CLI, that would be deserialized using a new `ObjectInputStream`, bypassing the existing blacklist-based protection mechanism. We're fixing this issue by adding `SignedObject` to the blacklist.

EVRS 88/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.997 99.95th percentile · FIRST	CISA DEADLINE Oct 23, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.997 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, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

We're also backporting the new HTTP CLI protocol from Jenkins 2.54 to LTS 2.46.2, and deprecating the remoting-based (i.e. Java serialization) CLI protocol, disabling it by default.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.jenkins-ci.main:jenkins-core	≥ 2.50, ≤ 2.56	2.57	GitHub
org.jenkins-ci.main:jenkins-core	≤ 2.46.1	2.46.2	GitHub
jenkins	≤ 2.56 ≤ 2.46.1	after 2.56 · after 2.46.1	NVD
communications cloud native core automated test suite	1.9.0	no fixed version listed	NVD

Sources

Vendor guidance oracle.com/security-alerts/cpuapr2022.html
jenkins.io jenkins.io/security/advisory/2017-04-26/
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-1921

Additional guidance jenkins.io/security/advisory/2017-04-26/
NVD nvd.nist.gov/vuln/detail/CVE-2017-1000353
GitHub advisory github.com/advisories/GHSA-26wc-3wqp-g3rp
Current data evulnable.com/vulnerability-management/cve/CVE-2017-1000353

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