

CVE-2018-1000861

Jenkins Stapler Web Framework Deserialization of Untrusted Data Vulnerability

Exigent CISA KEV since Feb 10, 2022 Actively exploited Public exploit module (Metasploit)

A code execution vulnerability exists in the Stapler web framework used by Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in stapler/core/src/main/java/org/kohsuke/stapler/MetaClass.java that allows attackers to invoke some methods on Java objects by accessing crafted URLs that were not intended to be invoked this way.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.983 99.92nd percentile · FIRST	CISA DEADLINE Aug 10, 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	0.983 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 updates per vendor instructions.
 Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
jenkins	≤ 2.138.3 ≤ 2.153	after 2.138.3 · after 2.153	NVD
openshift container platform	3.11	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-hhpm-5cp2-hg4x	Additional guidance	jenkins.io/security/advisory/2018-12-05/#SECURITY-595
NVD	nvd.nist.gov/vuln/detail/CVE-2018-1000861	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-4161	Current data	evulnable.com/vulnerability-management/cve/CVE-2018-1000861

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