

CVE-2020-10199

Sonatype Nexus Repository Remote Code Execution Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

Sonatype Nexus Repository before 3.21.2 allows JavaEL Injection (issue 1 of 2).

EVRS 85 /100 Immediate priority	CVSS V3.1 8.8 High · NVD	EPSS 0.991 99.93rd percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	0.991 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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
org.sonatype.nexus:nexus-extdirect	< 3.21.2	3.21.2	GitHub
nexus	< 3.21.2	3.21.2	NVD

Sources

Vendor guidance	support.sonatype.com/hc/en-us/articles/360044882533	NVD	nvd.nist.gov/vuln/detail/CVE-2020-10199
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-g2f6-v5qh-h2mq
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-0379	Current data	evulnable.com/vulnerability-management/cve/CVE-2020-10199

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