CVE-2019-7238

Sonatype Nexus Repository Manager Incorrect Access Control Vulnerability

CISA KEV since Dec 10, 2021 | Actively exploited

Sonatype Nexus Repository Manager before 3.15.0 has Incorrect Access Control.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
81/100	9.8	0.766	Jun 10, 2022
Urgent priority	Critical · NVD	99.55th percentile · FIRST	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	0.766 probability	− Pre-patch disclosure	Disclosure status unavailable
✓ CVSS	Base score 9.8	− Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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
nexus repository manager	⩾ 3.0.0 < 3.15.0	3.15.0	NVD

Sources

Vendor guidance support.sonatype.com/hc/en-us/articles/360017310793-CVE-2019-7238-Nexus-Repository-Manager-3-Missing-Access-Controls-and-Remote-Code-Execution-February-5th-2019

NVD nvd.nist.gov/vuln/detail/CVE-2019-7238

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-16782

Current data evulnable.com/vulnerability-management/cve/CVE-2019-7238

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