CVE-2020-10199

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-10199
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-01 19:15:00 UTC
Updated	2022-10-07 13:15:00 UTC
Description	Sonatype Nexus Repository before 3.21.2 allows JavaEL Injection (issue 1 of 2).

Risk And Classification

EPSS: 0.943790000 probability, percentile 0.999690000 (date 2026-04-12)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-917

CISA Known Exploited Vulnerability

Vendor	Sonatype
Product	Nexus Repository
Name	Sonatype Nexus Repository Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-10199

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sonatype	Nexus	All	All	All	All
Application	Sonatype	Nexus	All	All	All	All

References

Reference
CVE-2020-10199 Nexus Repository Manager 3 - Remote Code Execution - 2020-03-31 – Sonatype Support
Sonatype Nexus 3.21.1 Remote Code Execution ≈ Packet Storm
CWE - CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')
Nexus Repository Manager 3.21.1-01 Remote Code Execution – Packet Storm

Nexus Repository Manager 3.21.1-01 Remote Code Execution ≈ Packet Storm
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981903 Java (maven) Security Update for org.sonatype.nexus:nexus-extdirect (GHSA-g2f6-v5qh-h2mq)