

CVE-2021-21315

Npm package System Information Library for Node.JS Command Injection

CISA KEV since Jan 18, 2022

Actively exploited

The System Information Library for Node.JS (npm package "systeminformation") is an open source collection of functions to retrieve detailed hardware, system and OS information. In systeminformation before version 5.3.1 there is a command injection vulnerability. Problem was fixed in version 5.3.1. As a workaround instead of upgrading, be sure to check or sanitize service parameters that are passed to si.inetLatency(), si.inetChecksite(), si.services(), si.processLoad() ... do only allow strings, reject any arrays. String sanitation works as expected.

EVRS 82 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.907 99.81st percentile · FIRST	CISA DEADLINE Feb 1, 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	0.907 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ 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
systeminformation	< 5.3.1	5.3.1	GitHub
cordova	10.0.0	no fixed version listed	NVD

Sources

Vendor guidance	github.com/sebhildebrandt/systeminformation/commit/07daa05fb06f24f96297abaa30c2ace8bfd8b525	NVD	nvd.nist.gov/vuln/detail/CVE-2021-21315
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-2m8v-572m-ff2v
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-0527	Current data	evulnabile.com/vulnerability-management/cve/CVE-2021-21315

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