CVE-2023-32313

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

Summary

CVE	CVE-2023-32313
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-15 20:15:00 UTC
Updated	2023-05-24 20:43:00 UTC
Description	vm2 is a sandbox that can run untrusted code with Node's built-in modules. In versions 3.9.17 and lower of vm2 it was poss

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vm2 Project	Vm2	All	All	All	All

References

Reference	Source	Link	Tags
PoC for breaking console.log in vm2@3.9.17 · GitHub	MISC	gist.github.com	
Inspect method should be readonly · patriksimek/vm2@5206ba2 · GitHub	MISC	github.com	
Inspect Manipulation · Advisory · patriksimek/vm2 · GitHub	MISC	github.com	
Release 3.9.18 · patriksimek/vm2 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report