CVE-2022-36067

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

Summary

CVE	CVE-2022-36067
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-06 22:15:00 UTC
Updated	2022-11-08 03:03:00 UTC
Description	vm2 is a sandbox that can run untrusted code with whitelisted Node's built-in modules. In versions prior to version 3.9.11, a

Risk And Classification

Problem Types: CWE-913

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
CVE-2022-36067 NPM Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netap
Sandbox Breakout in VM2 · Issue #467 · patriksimek/vm2 · GitHub	MISC	github.com
Enter "Sandbreak" - Vulnerability In vm2 Sandbox Module Enables Remote Code Execution (CVE-2022-36067)	MISC	www.oxeye.io
Sandbox Escape · Advisory · patriksimek/vm2 · GitHub	CONFIRM	github.com
vm2/setup-sandbox.js at master · patriksimek/vm2 · GitHub	MISC	github.com
Fix 467 · patriksimek/vm2@d9a7f3c · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

377634 vm2 NPM Package Remote Code Execution (RCE) Vulnerability (GHSA-mrgp-mrhc-5jrq) (Sandbreak)