



CVE-2021-23449

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-23449
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-18 17:15:00 UTC
Updated	2022-06-28 14:11:00 UTC
Description	This affects the package vm2 before 3.9.4 via a Prototype Pollution attack vector, which can lead to execution of arbitrary c

Risk And Classification

Problem Types: CWE-1321

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
CVE-2021-23449 NPM Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Security Fixes · patriksimek/vm2@b4f6e2b · GitHub	MISC	github.com	
Prototype Pollution in vm2 Snyk	MISC	snyk.io	
Release 3.9.4 · patriksimek/vm2 · GitHub	MISC	github.com	
Sandbox breakout · Issue #363 · patriksimek/vm2 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Cris Staicu

LEGACY: Abdullah Alhamdan

Legacy QID Mappings

[375998](#) Node.js VM2 Module Arbitrary Code Execution Vulnerability

[980244](#) Nodejs (npm) Security Update for vm2 (GHSA-rjf2-j2r6-q8gr)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)