



CVE-2022-25893

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

Summary

CVE	CVE-2022-25893
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-21 05:15:00 UTC
Updated	2023-01-03 13:59:00 UTC
Description	The package vm2 before 3.9.10 are vulnerable to Arbitrary Code Execution due to the usage of prototype lookup for the We

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
Arbitrary Code Execution in vm2 CVE-2022-25893 Snyk	CONFIRM	security.snyk.io	
Security fix for issue 444. by XmiliaH · Pull Request #445 · patriksimek/vm2 · GitHub	CONFIRM	github.com	
Security Issue · Issue #444 · patriksimek/vm2 · GitHub	CONFIRM	github.com	
Security fix for issue 444. by XmiliaH · Pull Request #445 · patriksimek/vm2 · GitHub	CONFIRM	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: Ghaem Arasteh

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

© [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](#)