



CVE-2021-21374

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

Summary

CVE	CVE-2021-21374
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-26 22:15:00 UTC
Updated	2021-03-30 21:36:00 UTC
Description	Nimble is a package manager for the Nim programming language. In Nim release versions before versions 1.2.10 and 1.4.4

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nim-lang	Nim	All	All	All	All

References

Reference	Source	Link	T
basic cleanups regarding SSL handling by Araq · Pull Request #16940 · nim-lang/Nim · GitHub	MISC	github.com	
nimble/changelog.markdown at master · nim-lang/nimble · GitHub	MISC	github.com	
Nim - Insecure SSL/TLS Defaults, MitM, and nimble Remote Code Execution ConsenSys Diligence	MISC	consensys.net	
Nimble fails to validate certificates due to insecure httpClient defaults · Advisory · nim-lang/security · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180314](#) Debian Security Update for nim (CVE-2021-21374)

[750247](#) OpenSUSE Security Update for nim (openSUSE-SU-2021:0618-1)

© [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](#)