



CVE-2020-15690

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

Summary

CVE	CVE-2020-15690
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-30 06:15:00 UTC
Updated	2021-02-09 18:50:00 UTC
Description	In Nim before 1.2.6, the standard library asyncfpcclient lacks a check for whether a message contains a newline character.

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Nim - stdlib asyncfpc - Crlf Injection ConsenSys Diligence	MISC	consensys.net	Exploit
oss-security - [CVE-2020-15690] Nim - stdlib asyncfpc - Crlf Injection	MLIST	www.openwall.com	Exploit
pub/pocs/cve-2020-15690 at master · tintinweb/pub · GitHub	MISC	github.com	Exploit
Comparing v1.2.4...v1.2.6 · nim-lang/Nim · GitHub	CONFIRM	github.com	Patch
Nim/asyncfpcclient.nim at dc5a40f3f39c6ea672e6dc6aca7f8118a69dda99 · nim-lang/Nim · GitHub	MISC	github.com	Exploit
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180725](#) Debian Security Update for nim (CVE-2020-15690)

© [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](#)