



CVE-2021-3254

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

Summary

CVE	CVE-2021-3254
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-11 12:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	Asus DSL-N14U-B1 1.1.2.3_805 allows remote attackers to cause a Denial of Service (DoS) via a TCP SYN scan using nrr

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Asus	Dsl-n14u-b1	-	All	All	All
Operating System	Asus	Dsl-n14u-b1 Firmware	1.1.2.3_805	All	All	All

References

Reference	Source	Link
kaisersource.github.io/2021-01-22-dsl-n14u.md at main · kaisersource/kaisersource.github.io · GitHub	MISC	github.com
KaiserSource@home:~\$	MISC	kaisersource.github.io
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#).

CVE.report and Source URL Uptime Status status.cve.report