



CVE-2022-24372

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

Summary

CVE	CVE-2022-24372
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-27 18:15:00 UTC
Updated	2022-05-09 18:23:00 UTC
Description	Linksys MR9600 devices before 2.0.5 allow attackers to read arbitrary files via a symbolic link to the root directory of a NAS

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Linksys	Mr9600	-	All	All	All
Operating System	Linksys	Mr9600 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Linksys Dual-Band Mesh-WLAN WiFi 6 Router (MR9600)	MISC	www.linksys.com	
www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-046.txt	MISC	www.syss.de	
Linksys Dual-Band Mesh WiFi 6 Router (MR9600)	MISC	www.linksys.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#).

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