



CVE-2022-23900

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

Summary

CVE	CVE-2022-23900
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-07 11:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	A command injection vulnerability in the API of the Wavlink WL-WN531P3 router, version M31G3.V5030.201204, allows an

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Wavlink	WI-wn531p3	-	All	All	All
Operating System	Wavlink	WI-wn531p3 Firmware	m31g3.v5030.201204	All	All	All

References

Reference	Source	Link
WN531P3 – AC1200 Dual-band Smart Wi-Fi Router with Touchlink - WAVLINK See the world! Powered by Wavlink	MISC	www.wavl
Wavlink Command Injection (CVE-2022-23900) by Stigward Apr, 2022 Medium	MISC	stigward.n
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

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