CVE-2020-12125

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-12125
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-02 09:15:00 UTC
Updated	2020-10-08 01:14:00 UTC
Description	A remote buffer overflow vulnerability in the /cgi-bin/makeRequest.cgi endpoint of the WAVLINK WN530H4 M30H4.V5030.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Wavlink	Wn530h4	-	All	All	All
Hardware	Wavlink	Wn530h4	-	All	All	All
Operating System	Wavlink	Wn530h4 Firmware	m30h4.v5030.190403	All	All	All
Operating System	Wavlink	Wn530h4 Firmware	m30h4.v5030.190403	All	All	All

References

Reference	Source	Link
Christopher Cerne | CVE-2020-12125	MISC	cerne.xyz
WL-WN530H4 AC1200 High Power Dual Band Wireless Router - WAVLINK See the world! Powered by Wavlink	MISC	www.wavlink.
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.