CVE-2022-46424

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-46424
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-20 20:15:00 UTC
Updated	2023-11-07 03:55:00 UTC
Description	An exploitable firmware modification vulnerability was discovered on the Netgear XWN5001 Powerline 500 WiFi Access Po

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Xwn5001	-	All	All	All
Operating System	Netgear	Xwn5001 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Two Vulnerabilities Regarding Firmware Updates in Netgear XWN5001 WiFi Access Point - HackMD		hackmd.io	
www.netgear.com/about/security	MISC	www.netgear.com	
Two Vulnerabilities Regarding Firmware Updates in Netgear XWN5001 WiFi Access Point - HackMD	MISC	hackmd.io	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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

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