



CVE-2022-47519

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-47519
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-18 06:15:00 UTC
Updated	2023-11-07 03:56:00 UTC
Description	An issue was discovered in the Linux kernel before 6.0.11. Missing validation of IEEE80211_P2P_ATTR_OPER_CHANNEL

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference	Source	Link
[PATCH 2/4] wifi: wilc1000: validate length of IEEE80211_P2P_ATTR_OPER_CHANNEL attribute - Phil Turnbull		lore.kernel
wifi: wilc1000: validate length of IEEE80211_P2P_ATTR_OPER_CHANNEL at... · torvalds/linux@051ae66 · GitHub	MISC	github.com

December 2022 Linux Kernel 6.0.11 Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.n
[PATCH 2/4] wifi: wilc1000: validate length of IEEE80211_P2P_ATTR_OPER_CHANNEL attribute - Phil Turnbull	MISC	lore.kerne
[SECURITY] [DLA 3244-1] linux-5.10 security update	MLIST	lists.debia
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [181434](#) Debian Security Update for linux (CVE-2022-47519)
- [181440](#) Debian Security Update for linux-5.10 (DLA 3244-1)
- [199209](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5912-1)
- [199211](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5911-1)
- [199220](#) Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5929-1)
- [199223](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5935-1)
- [199227](#) Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5938-1)
- [199229](#) Ubuntu Security Notification for Linux kernel (KVM) Vulnerabilities (USN-5941-1)
- [199238](#) Ubuntu Security Notification for Linux kernel (KVM) Vulnerabilities (USN-5950-1)
- [199243](#) Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5962-1)
- [378468](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)
- [378512](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)
- [904729](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11867)
- [904736](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11857)
- [905197](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11867-1)
- [905890](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11867-2)
- [906260](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11857-2)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)