



CVE-2022-42719

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

Summary

CVE	CVE-2022-42719
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-13 23:15:00 UTC
Updated	2023-11-07 03:53:00 UTC
Description	A use-after-free in the mac80211 stack when parsing a multi-BSSID element in the Linux kernel 5.2 through 5.19.x before 5

Risk And Classification

Problem Types: CWE-416

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	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source
[SECURITY] Fedora 36 Update: kernel-5.19.15-201.fc36 - package-announce - Fedora Mailing-Lists	FEDORA
Kernel Live Patch Security Notice LNS-0091-1 ≈ Packet Storm	MISC
October 2022 Linux Kernel 5.19.15 Vulnerabilities in NetApp Products NetApp Product Security	CONF
oss-security - Various Linux Kernel WLAN security issues (RCE/DOS) found	MISC
oss-security - Re: Various Linux Kernel WLAN security issues (RCE/DOS) found	MISC
[SECURITY] Fedora 35 Update: kernel-5.19.15-101.fc35 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 37 Update: kernel-5.19.15-301.fc37 - package-announce - Fedora Mailing-Lists	FEDORA

[SECURITY] Fedora 37 Update: kernel-5.19.15-301.fc37 - package-announce - Fedora Mailing-Lists	
Debian -- Security Information -- DSA-5257-1 linux	DEB
[SECURITY] [DLA 3173-1] linux-5.10 security update	MLIS
[SECURITY] Fedora 36 Update: kernel-5.19.15-201.fc36 - package-announce - Fedora Mailing-Lists	
Bug 1204051 – VUL-0: CVE-2022-42719: kernel: remote crash/code execution with wlan frames when parsing a multi-BSSID element	MISC
kernel/git/wireless/wireless.git - kvalo's fork of linux.git	MISC
[SECURITY] Fedora 35 Update: kernel-5.19.15-101.fc35 - package-announce - Fedora Mailing-Lists	FED
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181145 Debian Security Update for linux (DSA 5257-1)
181190 Debian Security Update for linux-5.10 (DLA 3173-1)
184058 Debian Security Update for linux (CVE-2022-42719)
198997 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5692-1)
198999 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5693-1)
199006 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5700-1)
199014 Ubuntu Security Notification for backport-iwlwifi-dkms Vulnerabilities (USN-5708-1)
199029 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5728-1)
199037 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5728-2)
199051 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5728-3)
199053 Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-5752-1)
283201 Fedora Security Update for kernel (FEDORA-2022-2cfbe17910)
283209 Fedora Security Update for kernel (FEDORA-2022-b948fc3cfb)
283477 Fedora Security Update for kernel (FEDORA-2022-1a5b125ac6)
377891 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0002)
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)
502548 Alpine Linux Security Update for linux-lts

504122 Alpine Linux Security Update for linux-lts
610462 Google Android Devices January 2023 Security Patch Missing
610467 Google Android February 2023 Security Patch Missing for Samsung
752708 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3704-1)
752724 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3775-1)
752750 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3844-1)
752889 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3897-1)
752911 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3998-1)
753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
753119 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 15 for SLE 15 SP3) (SUSE-SU-2022:3657-1)
753143 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15 SP3) (SUSE-SU-2022:3606-1)
753150 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 2 for SLE 15 SP4) (SUSE-SU-2022:3605-1)
753339 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 3 for SLE 15 SP4) (SUSE-SU-2022:3601-1)
753352 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15 SP2) (SUSE-SU-2022:3648-1)
753374 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3809-1)
753375 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 1 for SLE 15 SP4) (SUSE-SU-2022:3628-1)
753394 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 30 for SLE 15 SP2) (SUSE-SU-2022:3607-1)
904238 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11164)
904248 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11138)
904369 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11164-1)
904424 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11138-1)
906059 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11164-2)
906431 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11138-2)

© 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](#)