



# CVE-2022-28389

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

## Summary

<b>CVE</b>	CVE-2022-28389
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-03 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:45:00 UTC
<b>Description</b>	mcba_usb_start_xmit in drivers/net/can/usb/mcba_usb.c in the Linux kernel through 5.17.1 has a double free.

## Risk And Classification

**Problem Types:** CWE-415

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500s</a>	-	All	All	All

Operating System	<a href="#">Netapp</a>	<a href="#">H500s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700s Firmware</a>	-	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 35 Update: kernel-5.16.19-200.fc35 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
can: mcba_usb: mcba_usb_start_xmit(): fix double dev_kfree_skb in err... · torvalds/linux@04c9b00 · GitHub	MISC	<a href="#">github.com</a>
[SECURITY] Fedora 34 Update: kernel-5.16.19-100.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: kernel-5.16.19-100.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
Debian -- Security Information -- DSA-5127-1 linux	DEBIAN	<a href="#">www.debian.org</a>
[SECURITY] Fedora 36 Update: kernel-5.17.2-300.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
Debian -- Security Information -- DSA-5173-1 linux	DEBIAN	<a href="#">www.debian.org</a>
[SECURITY] Fedora 36 Update: kernel-5.17.2-300.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
April 2022 Linux Kernel 5.17.1 Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>
[SECURITY] Fedora 35 Update: kernel-5.16.19-200.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">179258</a> Debian Security Update for linux (DSA 5127-1)
<a href="#">180605</a> Debian Security Update for linux (DSA 5173-1)
<a href="#">184218</a> Debian Security Update for linux (CVE-2022-28389)
<a href="#">198783</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5416-1)
<a href="#">198822</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5469-1)
<a href="#">198824</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5467-1)
<a href="#">198858</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5515-1)
<a href="#">282579</a> Fedora Security Update for kernel (FEDORA-2022-91633399ff)
<a href="#">282580</a> Fedora Security Update for kernel (FEDORA-2022-5cd9d787dc)
<a href="#">353293</a> Amazon Linux Security Advisory for kernel · ALAS2 2022 1793

353956 Amazon Linux Security Advisory for kernel : ALAS-2022-1591

355563 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-036

376925 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125)

377766 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2022:0049)

377871 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0001)

6140252 AWS Bottlerocket Security Update for kernel (GHSA-5jc4-vjq7-64w8)

671975 EulerOS Security Update for kernel (EulerOS-SA-2022-2159)

672003 EulerOS Security Update for kernel (EulerOS-SA-2022-2134)

752036 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1183-1)

752039 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1196-1)

752042 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1197-1)

752048 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1266-1)

752052 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1255-1)

752053 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1267-1)

752058 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1256-1)

753151 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15) (SUSE-SU-2022:2709-1)

753184 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 11 for SLE 15 SP3) (SUSE-SU-2022:2738-1)

753216 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 16 for SLE 15 SP3) (SUSE-SU-2022:2727-1)

753219 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 14 for SLE 15 SP3) (SUSE-SU-2022:2726-1)

753246 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15 SP1) (SUSE-SU-2022:2728-1)

753277 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 28 for SLE 15 SP1) (SUSE-SU-2022:2700-1)

753319 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 7 for SLE 15 SP3) (SUSE-SU-2022:2766-1)

753346 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 21 for SLE 15 SP2) (SUSE-SU-2022:2783-1)

753373 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1257-1)

753417 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1163-1)

753427 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1407-1)

753443 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15 SP2) (SUSE-SU-2022:2776-1)

753481 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 9 for SLE 15 SP3) (SUSE-SU-2022:2770-1)

753491 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP4) (SUSE-SU-2022:2854-1)
900800 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9282)
901124 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9294)
901334 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9282-1)
902121 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9294-1)
905848 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9282-2)
906510 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9294-2)

© [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](#)**