



CVE-2021-38204

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

Summary

CVE	CVE-2021-38204
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-08 20:15:00 UTC
Updated	2022-01-04 16:37:00 UTC
Description	drivers/usb/host/max3421-hcd.c in the Linux kernel before 5.13.6 allows physically proximate attackers to cause a denial of

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	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
usb: max-3421: Prevent corruption of freed memory · torvalds/linux@b5fdf5c · GitHub	MISC	github.com	
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.6	MISC	cdn.kernel.org	
[SECURITY] [DLA 2843-1] linux security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178943](#) Debian Security Update for linux (DLA 2843-1)

[179766](#) Debian Security Update for linux (CVE-2021-38204)

[198514](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5091-1)

198515 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-1)
198518 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5094-2)
198520 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5094-1)
198521 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5091-2)
198523 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-2)
198524 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5096-1)
198542 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5115-1)
352871 Amazon Linux Security Advisory for kernel : ALAS-2021-1539
353097 Amazon Linux Security Advisory for kernel : ALAC2012-2021-033
353098 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-034
353099 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-035
610386 Google Android Devices December 2021 Security Patch Missing
610392 Google Android January 2022 Security Patch Missing for Huawei EMUI
751137 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1271-1)
751155 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3192-1)
751160 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3179-1)
751163 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3206-1)
751170 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3205-1)
751437 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3876-1)
751441 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3876-1)
751451 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3935-1)
751473 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3969-1)
751476 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3972-1)
900294 CBL-Mariner Linux Security Update for kernel 5.10.52.1
900304 CBL-Mariner Linux Security Update for kernel 5.10.57.1
900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1
900968 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6588-1)
903591 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5079)

© [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](#)