



CVE-2021-38205

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

Summary

CVE	CVE-2021-38205
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 16:38:00 UTC
Description	drivers/net/ethernet/xilinx/xilinx_emaclite.c in the Linux kernel before 5.13.3 makes it easier for attackers to defeat an ASLR

Risk And Classification

Problem Types: CWE-824

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
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.3	MISC	cdn.kernel.org	
[SECURITY] [DLA 2785-1] linux-4.19 security update	MLIST	lists.debian.org	
[SECURITY] [DLA 2843-1] linux security update	MLIST	lists.debian.org	
net: xilinx_emaclite: Do not print real IOMEM pointer · torvalds/linux@d0d62ba · GitHub	MISC	github.com	
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

[178844](#) Debian Security Update for linux-4.19 (DLA 2785-1)

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

180189 Debian Security Update for linux (CVE-2021-38205)
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)
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)
198544 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5116-1)
198546 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5116-2)
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
356186 Amazon Linux Security Advisory for microvm-kernel : ALASMICROVM-KERNEL-4.14-2023-003
356218 Amazon Linux Security Advisory for microvm-kernel : ALASMICROVM-KERNEL-4.14-2023-002
671134 EulerOS Security Update for kernel (EulerOS-SA-2021-2688)
671137 EulerOS Security Update for kernel (EulerOS-SA-2021-2713)
751137 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1271-1)
751160 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3179-1)
751170 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3205-1)
900294 CBL-Mariner Linux Security Update for kernel 5.10.52.1
900302 CBL-Mariner Linux Security Update for kernel 5.10.57.1
900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1
901572 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6589-1)
903118 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5080)
905873 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5080-1)

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](#)