



CVE-2021-29264

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

Summary

CVE	CVE-2021-29264
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-26 22:15:00 UTC
Updated	2022-05-27 16:47:00 UTC
Description	An issue was discovered in the Linux kernel through 5.11.10. drivers/net/ethernet/freescale/gianfar.c in the Freescale Gianfar

Risk And Classification

Problem Types: NVD-CWE-Other

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
[SECURITY] [DLA 2690-1] linux-4.19 security update	MLIST	lists.debian.org	
kernel/git/stable/linux.git - Linux kernel stable tree	MISC	git.kernel.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

[174896](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1177-1)

[174897](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1175-1)

[174916](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1210-1)

[174917](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1211-1)

174919	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1238-1)
178679	Debian Security Update for linux-4.19 (DLA 2690-1)
179118	Debian Security Update for linux (DLA 2940-1)
180269	Debian Security Update for linux (CVE-2021-29264)
198365	Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4948-1)
198366	Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4949-1)
198371	Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4946-1)
198401	Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4982-1)
281395	Fedora Security Update for kernel (FEDORA-2021-41fb54ae9f)
281396	Fedora Security Update for kernel (FEDORA-2021-2306e89112)
281397	Fedora Security Update for kernel (FEDORA-2021-6b0f287b8b)
353242	Amazon Linux Security Advisory for kernel : ALAC2012-2022-036
353243	Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2022-037
353244	Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2022-038
670416	EulerOS Security Update for kernel (EulerOS-SA-2021-1983)
670438	EulerOS Security Update for kernel (EulerOS-SA-2021-2062)
670449	EulerOS Security Update for kernel (EulerOS-SA-2021-2051)
750004	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1573-1)
750006	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1596-1)
750014	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1623-1)
750015	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1624-1)
750199	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0758-1)
750276	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0532-1)
750650	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)
750652	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)
750762	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)
750766	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)
900100	CBL-Mariner Linux Security Update for kernel 5.10.52.1

900305 CBL-Mariner Linux Security Update for kernel 5.10.57.1
900320 CBL-Mariner Linux Security Update for kernel 5.10.60.1
901061 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6546-1)
903514 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4025)
906144 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4025-1)

© [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](#)