



CVE-2022-0854

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

Summary

CVE	CVE-2022-0854
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-23 20:15:00 UTC
Updated	2022-10-14 12:53:00 UTC
Description	A memory leak flaw was found in the Linux kernel's DMA subsystem, in the way a user calls DMA_FROM_DEVICE. This fl

Risk And Classification

Problem Types: CWE-401

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	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	5.17	-	All	All
Operating System	Linux	Linux Kernel	5.17	rc1	All	All
Operating System	Linux	Linux Kernel	5.17	rc2	All	All
Operating System	Linux	Linux Kernel	5.17	rc3	All	All
Operating System	Linux	Linux Kernel	5.17	rc4	All	All
Operating System	Linux	Linux Kernel	5.17	rc5	All	All
Operating System	Linux	Linux Kernel	5.17	rc6	All	All
Operating System	Linux	Linux Kernel	5.17	rc7	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-5173-1 linux	DEBIAN	www.debian.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	

[SECURITY] [DLA 3065-1] linux security update	MLIST	lists.debian.org	
Debian -- Security Information -- DSA-5161-1 linux	DEBIAN	www.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

160210 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-7683)
160270 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-8267)
179371 Debian Security Update for linux (DSA 5161-1)
180282 Debian Security Update for linux (DLA 3065-1)
180605 Debian Security Update for linux (DSA 5173-1)
182936 Debian Security Update for linux (CVE-2022-0854)
198747 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5381-1)
240815 Red Hat Update for kernel-rt (RHSA-2022:7444)
240817 Red Hat Update for kernel security (RHSA-2022:7683)
240869 Red Hat Update for kernel-rt (RHSA-2022:7933)
240904 Red Hat Update for kernel security (RHSA-2022:8267)
242855 Red Hat Update for kernel (RHSA-2024:0412)
353947 Amazon Linux Security Advisory for kernel : ALAS2-2022-1798
353956 Amazon Linux Security Advisory for kernel : ALAS-2022-1591
353960 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-014
353962 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-026
354468 Amazon Linux Security Advisory for kernel : ALAS2022-2022-185
354499 Amazon Linux Security Advisory for kernel : ALAS2022-2022-042
354542 Amazon Linux Security Advisory for kernel : ALAS-2022-185
355199 Amazon Linux Security Advisory for kernel : ALAS2023-2023-070
6140139 AWS Bottlerocket Security Update for kernel (GHSA-2cx3-x92j-3jrp)
671804 EulerOS Security Update for kernel (EulerOS-SA-2022-1844)

671929 EulerOS Security Update for kernel (EulerOS-SA-2022-1999)
671975 EulerOS Security Update for kernel (EulerOS-SA-2022-2159)
672003 EulerOS Security Update for kernel (EulerOS-SA-2022-2134)
672016 EulerOS Security Update for kernel (EulerOS-SA-2022-2273)
752036 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1183-1)
752042 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1197-1)
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)
900782 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9139)
901090 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9142)
902125 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9142-1)
902690 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9139-1)
906030 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9139-2)
906373 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9142-2)
940732 AlmaLinux Security Update for kernel (ALSA-2022:7683)
940766 AlmaLinux Security Update for kernel-rt (ALSA-2022:7444)
940798 AlmaLinux Security Update for kernel (ALSA-2022:8267)
940843 AlmaLinux Security Update for kernel-rt (ALSA-2022:7933)
960176 Rocky Linux Security Update for kernel-rt (RLSA-2022:7444)
960184 Rocky Linux Security Update for kernel (RLSA-2022:7683)

© [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](#)