CVE-2022-3108

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-3108
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-14 21:15:00 UTC
Updated	2022-12-16 21:39:00 UTC
Description	An issue was discovered in the Linux kernel through 5.16-rc6. kfd_parse_subtype_iolink in drivers/gpu/drm/amd/amdkfd/kfc

Risk And Classification

Problem Types: CWE-252

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.16.0	-	All	All
Operating System	Linux	Linux Kernel	5.16.0	rc1	All	All
Operating System	Linux	Linux Kernel	5.16.0	rc2	All	All
Operating System	Linux	Linux Kernel	5.16.0	rc3	All	All
Operating System	Linux	Linux Kernel	5.16.0	rc4	All	All
Operating System	Linux	Linux Kernel	5.16.0	rc5	All	All
Operating System	Linux	Linux Kernel	5.16.0	rc6	All	All

References

Reference	Source	Link	Tags
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
2153052 – (CVE-2022-3108) CVE-2022-3108 Kernel: kmemdup's return value not checked	MISC	bugzilla.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160551 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2023-12256)

160554 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12255)

184115 Debian Security Update for linux (CVE-2022-3108)

199301 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6027-1)

199356 Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6093-1)

199465 Ubuntu Security Notification for Linux kernel (Xilinx ZynqMP) Vulnerabilities (USN-6222-1)

199614 Ubuntu Security Notification for Linux kernel (IoT) Vulnerabilities (USN-6256-1)

378473 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0021)

378892 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0114)

379043 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)

672747 EulerOS Security Update for kernel (EulerOS-SA-2023-1469)

672802 EulerOS Security Update for kernel (EulerOS-SA-2023-1551)

672806 EulerOS Security Update for kernel (EulerOS-SA-2023-1526)

753562 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0134-1)

753564 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0147-1)

753565 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0146-1)

753566 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0145-1)

753583 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0152-1)

753584 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0149-1)

753688 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0406-1)

753689 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0410-1)

753743 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0618-1)

904691 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11634)

904703 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11609)

906369 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11609-2)

© 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 registred 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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**