



CVE-2022-47929

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

Summary

CVE	CVE-2022-47929
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-17 21:15:00 UTC
Updated	2023-05-03 14:15:00 UTC
Description	In the Linux kernel before 6.1.6, a NULL pointer dereference bug in the traffic control subsystem allows an unprivileged use

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3349-1] linux-5.10 security update	MLIST	lists.debian.org	
noqueue qdisc and non-virtual interfaces — Netdev	MISC	www.spinics.net	
Debian -- Security Information -- DSA-5324-1 linux	DEBIAN	www.debian.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	
[SECURITY] [DLA 3403-1] linux security update	MLIST	lists.debian.org	
Components of Linux Traffic Control	MISC	tldp.org	
cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.1.6	CONFIRM	cdn.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 OID Mappings

160505 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12196)
160506 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12199)
160508 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2023-12200)
160515 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2023-12207)
160516 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12206)
160583 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-2458)
160692 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-2951)
181491 Debian Security Update for linux (DSA 5324-1)
181618 Debian Security Update for linux-5.10 (DLA 3349-1)
181768 Debian Security Update for linux (DLA 3403-1)
183557 Debian Security Update for linux (CVE-2022-47929)
199208 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5915-1)
199212 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5917-1)
199218 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5927-1)
199224 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5934-1)
199226 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5939-1)
199230 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5940-1)
199239 Ubuntu Security Notification for Linux kernel (IBM) Vulnerabilities (USN-5951-1)
199261 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5984-1)
199267 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5991-1)
199276 Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6000-1)
199292 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6025-1)
199294 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6024-1)
199300 Ubuntu Security Notification for Linux kernel (Qualcomm Snapdragon) Vulnerabilities (USN-6030-1)
199303 Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-6040-1)
199321 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6057-1)
199385 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6134-1)
199502 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5975-1)

199541 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5924-1)
199560 Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6001-1)
199568 Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6013-1)
199570 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5981-1)
199577 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6014-1)
199587 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-6009-1)
199607 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6247-1)
199610 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6248-1)
241417 Red Hat Update for kernel security (RHSA-2023:2458)
241468 Red Hat Update for kernel-rt (RHSA-2023:2148)
241504 Red Hat Update for kernel security (RHSA-2023:2951)
241527 Red Hat Update for kernel-rt (RHSA-2023:2736)
242855 Red Hat Update for kernel (RHSA-2024:0412)
354736 Amazon Linux Security Advisory for kernel : ALAS2-2023-1932
354739 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-013
354741 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-026
354775 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-042
378473 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0021)
378537 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0048)
378710 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)
6140229 AWS Bottlerocket Security Update for kernel (GHSA-4gr8-53jw-hp89)
672707 EulerOS Security Update for kernel (EulerOS-SA-2023-1444)
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)
672876 EulerOS Security Update for kernel (EulerOS-SA-2023-1614)
672914 EulerOS Security Update for kernel (EulerOS-SA-2023-1781)
672951 EulerOS Security Update for kernel (EulerOS-SA-2023-1759)
672952 EulerOS Security Update for kernel (EulerOS-SA-2023-1759)

673117 EulerOS Security Update for kernel (EulerOS-SA-2023-2152)
753583 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0152-1)
753684 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0394-1)
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)
753692 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0407-1)
753709 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0433-1)
753743 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0618-1)
753745 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0634-1)
755900 SUSE Enterprise Linux Security Update for the Linux-RT Kernel (SUSE-SU-2023:0488-1)
905286 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13039)
905293 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13050)
905328 Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (13123)
905527 Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (13123-1)
905910 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13039-2)
906406 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13050-2)
941023 AlmaLinux Security Update for kernel (ALSA-2023:2458)
941061 AlmaLinux Security Update for kernel-rt (ALSA-2023:2148)
941096 AlmaLinux Security Update for kernel (ALSA-2023:2951)
941114 AlmaLinux Security Update for kernel-rt (ALSA-2023:2736)

© [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](#)