



CVE-2022-36280

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

Summary

CVE	CVE-2022-36280
State	PUBLIC
Assigner	security@openanolis.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-09 15:15:00 UTC
Updated	2023-05-03 14:15:00 UTC
Description	An out-of-bounds(OOB) memory access vulnerability was found in vmwgfx driver in drivers/gpu/vmxgfx/vmxgfx_kms.c in GL

Risk And Classification

Problem Types: CWE-787

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
Bug Access Denied	MISC	bugzilla.openanolis.cn	
[SECURITY] [DLA 3349-1] linux-5.10 security update	MLIST	lists.debian.org	
Debian -- Security Information -- DSA-5324-1 linux	DEBIAN	www.debian.org	
[SECURITY] [DLA 3403-1] linux security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Ziming Zhang(ezrakiez@gmail.com) from Ant Group Light-Year Security Lab

Legacy QID Mappings

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)
184909 Debian Security Update for linux (CVE-2022-36280)
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)
199255 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5976-1)
199260 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5982-1)
199261 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5984-1)
199265 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5987-1)
199267 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5991-1)
199276 Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6000-1)
199280 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6004-1)
199297 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6032-1)
199300 Ubuntu Security Notification for Linux kernel (Qualcomm Snapdragon) Vulnerabilities (USN-6030-1)
199343 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6079-1)
199353 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6091-1)
199354 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6096-1)
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)
378701	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0030)
378710	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)
379043	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)
672935	EulerOS Security Update for kernel (EulerOS-SA-2023-1824)
673208	EulerOS Security Update for kernel (EulerOS-SA-2023-2315)
673393	EulerOS Security Update for kernel (EulerOS-SA-2023-2647)
674113	EulerOS Security Update for kernel (EulerOS-SA-2023-2689)
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)
753807	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0768-1)
753808	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0778-1)
753810	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0780-1)
753832	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0852-1)
755842	SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2023:0774-1)
755851	SUSE Enterprise Linux Security Update for the linux kernel (SUSE-SU-2023:2646-1)
755900	SUSE Enterprise Linux Security Update for the Linux-RT Kernel (SUSE-SU-2023:0488-1)
903907	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10950)
906230	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10950-2)
906608	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10950-4)

© 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](#)