



CVE-2023-0030

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

Summary

CVE	CVE-2023-0030
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-08 23:15:00 UTC
Updated	2023-04-13 17:15:00 UTC
Description	A use-after-free flaw was found in the Linux kernel's nouveau driver in how a user triggers a memory overflow that causes t

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
2157270 – (CVE-2023-0030) CVE-2023-0030 kernel: Use after Free in nvkm_vmm_pfn_map	MISC	bugzilla.redhat.co
CVE-2023-0030 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.co
drm/nouveau/mmu: add more general vmm free/node handling functions · torvalds/linux@729eba3 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[181579](#) Debian Security Update for linux (CVE-2023-0030)

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

© [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](#)