CVE-2021-20292

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

Summary

CVE	CVE-2021-20292
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-28 11:15:00 UTC
Updated	2023-07-28 19:35:00 UTC
Description	There is a flaw reported in the Linux kernel in versions before 5.9 in drivers/gpu/drm/nouveau/nouveau_sgdma.c in nouveau

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

References

Reference	Source
[SECURITY] [DLA 2689-1] linux security update	MLIST
1939686 – (CVE-2021-20292) CVE-2021-20292 kernel: DRM Memory Management Double Free Privilege Escalation Vulnerability	MISC
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160345 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-10065)

178680 Debian Security Update for linux (DLA 2689-1)

179930 Debian Security Update for linux (CVE-2021-20292)

198371 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4946-1)

353242 Amazon Linux Security Advisory for kernel : ALAC2012-2022-036

353243 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2022-037

353244 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2022-038

390269 Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0031)

610372 Google Pixel Android October 2021 Security Patch Missing

670345 EulerOS Security Update for kernel (EulerOS-SA-2021-1879)

670438 EulerOS Security Update for kernel (EulerOS-SA-2021-2062)

670449 EulerOS Security Update for kernel (EulerOS-SA-2021-2051)

670463 EulerOS Security Update for kernel (EulerOS-SA-2021-2221)

670634 EulerOS Security Update for kernel (EulerOS-SA-2021-2392)

671047 EulerOS Security Update for kernel (EulerOS-SA-2021-2588)

752120 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1651-1)

752125 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1686-1)

752126 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1687-1)

752231 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2082-1)

752237 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2083-1)

752240 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2103-1)

752250 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2111-1)

753176 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1676-1)

753299 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1669-1)

© 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**