



CVE-2020-27820

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

Summary

CVE	CVE-2020-27820
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-03 00:15:00 UTC
Updated	2024-01-30 20:48:00 UTC
Description	A vulnerability was found in Linux kernel, where a use-after-frees in nouveau's postclose() handler could happen if removing

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	-	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc6	All	All
Application	Oracle	Communications Cloud Native Core Binding Support Function	22.1.3	All	All	All
Application	Oracle	Communications Cloud Native Core Network Exposure Function	22.1.1	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	22.2.0	All	All	All

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	MISC	bugzilla.redhat.com	
IPATCH 3/31 drm/nouveau: clean up all clients on device removal - Jeremy Cline	MISC	lore.kernel.org	

[PATCH 1/3] drm/nouveau: use drm_dev_unplug() during device removal - Jeremy Cline	MISC	lore.kernel.org	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
[PATCH 2/3] drm/nouveau: Add a dedicated mutex for the clients list - Jeremy Cline	MISC	lore.kernel.org	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
[PATCH 1/3] drm/nouveau: use drm_dev_unplug() during device removal - Jeremy Cline	MISC	lore.kernel.org	
[PATCH 2/3] drm/nouveau: Add a dedicated mutex for the clients list - Jeremy Cline	MISC	lore.kernel.org	
[PATCH 3/3] drm/nouveau: clean up all clients on device removal - Jeremy Cline	MISC	lore.kernel.org	
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159825 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-1988)
198653 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5265-1)
198659 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5278-1)
198785 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5415-1)
240275 Red Hat Update for kernel-rt (RHSA-2022:1975)
240298 Red Hat Update for kernel security (RHSA-2022:1988)
353141 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-010
353152 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-008
671448 EulerOS Security Update for kernel (EulerOS-SA-2022-1450)
671631 EulerOS Security Update for kernel (EulerOS-SA-2022-1661)
751590 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0056-1)
751600 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0068-1)
751602 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0080-1)
751622 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0131-1)
751654 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0197-1)
751695 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0367-1)

751697 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0366-1)
751701 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0366-1)
751702 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0371-1)
751989 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0131-1)
753264 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0079-1)
753355 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0056-1)
753441 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:14905-1)
940517 AlmaLinux Security Update for kernel (ALSA-2022:1988)

© [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](#)