



CVE-2021-3348

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-3348
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-01 04:15:00 UTC
Updated	2022-04-26 16:17:00 UTC
Description	nbd_add_socket in drivers/block/nbd.c in the Linux kernel through 5.10.12 has an nbd_queue_rq use-after-free that could b

Risk And Classification

Problem Types: CWE-362 | 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	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 2610-1] linux-4.19 security update	MLIST	lists.debian.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Mailing List, P
oss-security - Linux kernel: linux-block: nbd: use-after-free Read in nbd_queue_rq	MISC	www.openwall.com	Mailing List, P
oss-security - Re: Re: Linux kernel: linux-block: nbd: use-after-free Read in nbd_queue_rq	MLIST	www.openwall.com	Mailing List, P
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159492](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)

[178507](#) Debian Security Update for linux-4.19 (DLA 2610-1)

179955 Debian Security Update for linux (CVE-2021-3348)
198304 Ubuntu Security Notification for Linux-oem-5.10 Vulnerabilities (USN-4884-1)
198324 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4907-1)
198325 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4909-1)
198326 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4910-1)
239816 Red Hat Update for kernel security (RHSA-2021:4356)
239879 Red Hat Update for kernel-rt (RHSA-2021:4140)
353131 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-020
377055 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2021:0027)
6140370 AWS Bottlerocket Security Update for kernel (GHSA-qrpq-fg62-m5cm)
670345 EulerOS Security Update for kernel (EulerOS-SA-2021-1879)
670375 EulerOS Security Update for kernel (EulerOS-SA-2021-1950)
670396 EulerOS Security Update for kernel (EulerOS-SA-2021-1929)
670936 EulerOS Security Update for kernel (EulerOS-SA-2021-1929)
750373 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0241-1)
900098 CBL-Mariner Linux Security Update for kernel 5.4.91
903076 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3857)
940265 AlmaLinux Security Update for kernel (ALSA-2021:4356)

© [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](#)