



CVE-2020-25284

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

Summary

CVE	CVE-2020-25284
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-13 18:15:00 UTC
Updated	2022-04-28 18:32:00 UTC
Description	The rbd block device driver in drivers/block/rbd.c in the Linux kernel through 5.8.9 used incomplete permission checking for

Risk And Classification

Problem Types: CWE-863

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	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source	Link	Tags
grsecurity on Twitter: "https://t.co/shd29q7E1f"	MISC	twitter.com	Third Party Advisory
[security-announce] openSUSE-SU-2020:1655-1: important: Security update	SUSE	lists.opensuse.org	
[SECURITY] [DLA 2420-2] linux regression update	MLIST	lists.debian.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Patch, Vendor Advisory
[SECURITY] [DLA 2385-1] linux-4.19 security update	MLIST	lists.debian.org	Third Party Advisory
[SECURITY] [DLA 2420-1] linux security update	MLIST	lists.debian.org	
[security-announce] openSUSE-SU-2020:1586-1: important: Security update	SUSE	lists.opensuse.org	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159185 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1578)
239314 Red Hat Update for kernel-rt (RHSA-2021:1739)
239339 Red Hat Update for kernel (RHSA-2021:1578)
352338 Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-030
352339 Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-029
352340 Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-028
353135 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-016
377038 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)
6140166 AWS Bottlerocket Security Update for kernel (GHSA-78fq-9g2p-pjq4)
750376 OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
900076 CBL-Mariner Linux Security Update for kernel 5.4.91
903477 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3488)
905822 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3488-1)
940354 AlmaLinux Security Update for kernel (ALSA-2021:1578)

© [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](#)