



CVE-2020-28374

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

Summary

CVE	CVE-2020-28374
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-13 04:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
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	All

References

Reference	Source	Link
-----------	--------	------

[SECURITY] [DLA 2557-1] linux-4.19 security update	MLIST	lists.debian.org
[SECURITY] [DLA 2586-1] linux security update	MLIST	lists.debian.org
oss-security - Re: CVE-2020-28374: Linux SCSI target (LIO) unrestricted copy offload	MLIST	www.openwall.co
[SECURITY] Fedora 33 Update: kernel-headers-5.10.7-200.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
CVE-2020-28374 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.co
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
Debian -- Security Information -- DSA-4843-1 linux	DEBIAN	www.debian.org
Kernel Live Patch Security Notice LSN-0074-1 ≈ Packet Storm	MISC	packetstormsecur
[SECURITY] Fedora 33 Update: tcmu-runner-1.5.2-7.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject
oss-security - Re: CVE-2020-28374: Linux SCSI target (LIO) unrestricted copy offload	MLIST	www.openwall.co
scsi: target: Fix XCOPY NAA identifier lookup · torvalds/linux@2896c93 · GitHub	CONFIRM	github.com
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.10.7	CONFIRM	cdn.kernel.org
bugzilla.suse.com/attachment.cgi	MISC	bugzilla.suse.com
[SECURITY] Fedora 33 Update: kernel-headers-5.10.7-200.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject
[SECURITY] Fedora 32 Update: kernel-5.10.7-100.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject
[SECURITY] Fedora 33 Update: tcmu-runner-1.5.2-7.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
Bug 1178372 – VUL-0: CVE-2020-28374: kernel-source: LIO security issue	MISC	bugzilla.suse.com
[SECURITY] Fedora 32 Update: kernel-5.10.7-100.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
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

- [159144](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1093)
- [159277](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9306)
- [159278](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9307)
- [174805](#) SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 0 for SLE 15 SP2) (SUSE-SU-2021:0849-1)
- [174806](#) SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 39 for SLE 12 SP2) (SUSE-SU-2021:0835-1)
- [174807](#) SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 7 for SLE 15 SP2) (SUSE-SU-2021:0842-1)
- [174808](#) SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 36 for SLE 12 SP2) (SUSE-SU-2021:0870-1)
- [174809](#) SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 0 for SLE 15 SP2) (SUSE-SU-2021:0849-1)
- [174810](#) SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 19 for SLE 15 SP1) (SUSE-SU-2021:0853-1)

174812 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 13 for SLE 15 SP1) (SUSE-SU-2021:0859-1)
174813 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 5 for SLE 12 SP5) (SUSE-SU-2021:0818-1)
174817 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 8 for SLE 15 SP2) (SUSE-SU-2021:0841-1)
174819 SUSE Enterprise Linux Security update for the Linux Kernel (Live Patch 18 for SLE 15) (SUSE-SU-2021:0868-1)
239151 Red Hat Update for kernel (RHSA-2021:0856)
239174 Red Hat Update for kpatch-patch (RHSA-2021:0862)
239202 Red Hat Update for kernel (RHSA-2021:1093)
239204 Red Hat Update for kernel-rt (RHSA-2021:1081)
239254 Red Hat Update for kpatch-patch (RHSA-2021:1377)
239255 Red Hat Update for kernel (RHSA-2021:1376)
239343 Red Hat Update for kpatch-patch (RHSA-2021:1532)
239344 Red Hat Update for kernel (RHSA-2021:1531)
239349 Red Hat Update for kernel (RHSA-2021:2106)
239351 Red Hat Update for kpatch-patch (RHSA-2021:2099)
239374 Red Hat Update for kernel (RHSA-2021:2185)
239380 Red Hat Update for kpatch-patch (RHSA-2021:2167)
239453 Red Hat Update for kernel-rt (RHSA-2021:2190)
257070 CentOS Security Update for kernel (CESA-2021:0856)
352330 Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-038
352331 Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-037
352332 Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-036
352333 Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-035
353100 Amazon Linux Security Advisory for kernel : ALAC2012-2021-024
353101 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025
353102 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026
353132 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-019
377055 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2021:0027)
390233 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0005)
6140039 AWS Bottlerocket Security Update for kernel (GHSA-278i-xcri-6ah7)

670578 EulerOS Security Update for kernel (EulerOS-SA-2021-2336)
750428 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0075-1)
750434 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0060-1)
900040 CBL-Mariner Linux Security Update for kernel 5.4.91
902914 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3735)
906091 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3735-1)
940387 AlmaLinux Security Update for kernel (ALSA-2021:1093)

© [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](#)