



CVE-2021-27363

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

Summary

CVE	CVE-2021-27363
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-07 04:15:00 UTC
Updated	2022-05-23 16:00:00 UTC
Description	An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of f

Risk And Classification

Problem Types: NVD-CWE-noinfo

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
Application	Netapp	Cloud Backup	-	All	All	All
Operating System	Netapp	Solidfire Baseboard Management Controller Firmware	-	All	All	All

References

Reference	Source
New Old Bugs in the Linux Kernel	MISC
[SECURITY] [DLA 2586-1] linux security update	MLIST
oss-security - Linux iscsi security fixes	MISC
[SECURITY] [DLA 2610-1] linux-4.19 security update	MLIST
Bug 1182716 – VUL-0: CVE-2021-27363: kernel-source: show_transport_handle() shows iSCSI transport handle to non-root users	MISC
Kernel Live Patch Security Notice LSN-0075-1 ≈ Packet Storm	MISC
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC
March 2021 Linux Kernel 5.11.3 Vulnerabilities in NetApp Products NetApp Product Security	CONFIF
CVE Program record	CVE.OF

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159135](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9140)
- [159136](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9141)
- [159141](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1071)
- [159144](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1093)
- [159155](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9164)
- [159157](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9172)
- [159158](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9175)
- [174874](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 38 for SLE 12 SP3) (SUSE-SU-2021:1074-1)
- [174876](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 5 for SLE 12 SP5) (SUSE-SU-2021:1075-1)
- [174896](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1177-1)
- [174897](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1175-1)
- [174916](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1210-1)
- [174917](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1211-1)
- [174919](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1238-1)
- [174996](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:14724-1)
- [178507](#) Debian Security Update for linux-4.19 (DLA 2610-1)
- [179569](#) Debian Security Update for linux (CVE-2021-27363)
- [198303](#) Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-hwe, Linux-azure, Linux-azure-4.15, Linux-gcp, (USN-4883-1)
- [198307](#) Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-5.4, Linux-azure, Linux-azure-5.4, Linux-gcp, (USN-4887-1)
- [239202](#) Red Hat Update for kernel (RHSA-2021:1093)
- [239204](#) Red Hat Update for kernel-rt (RHSA-2021:1081)
- [239208](#) Red Hat Update for kernel-rt (RHSA-2021:1070)
- [239214](#) Red Hat Update for kernel (RHSA-2021:1171)
- [239217](#) Red Hat Update for kernel (RHSA-2021:1071)

239238 Red Hat Update for kernel (RHSA-2021:1272)
239255 Red Hat Update for kernel (RHSA-2021:1376)
239344 Red Hat Update for kernel (RHSA-2021:1531)
239455 Red Hat Update for kernel-rt (RHSA-2021:1279)
257073 CentOS Security Update for kernel (CESA-2021:1071)
352244 Amazon Linux Security Advisory for kernel: ALAS-2021-1487
352254 Amazon Linux Security Advisory for kernel: ALAS2-2021-1616
352324 Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-044
352325 Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-043
352326 Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-042
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
353150 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-001
390232 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0008)
6140418 AWS Bottlerocket Security Update for kernel (GHSA-mxrv-mrmf-6ccr)
670269 EulerOS Security Update for kernel (EulerOS-SA-2021-1808)
670320 EulerOS Security Update for kernel (EulerOS-SA-2021-1904)
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)
670634 EulerOS Security Update for kernel (EulerOS-SA-2021-2392)
670936 EulerOS Security Update for kernel (EulerOS-SA-2021-1929)
750004 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1573-1)
750006 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1596-1)
750014 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1623-1)
750015 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1624-1)
750199 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0758-1)
750276 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0532-1)

750650 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)
750652 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)
750762 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)
750766 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)
900101 CBL-Mariner Linux Security Update for kernel 5.10.52.1
900303 CBL-Mariner Linux Security Update for kernel 5.10.57.1
900321 CBL-Mariner Linux Security Update for kernel 5.10.60.1
901631 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6532-1)
903348 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3952)
906154 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3952-1)
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](#)