



CVE-2021-31916

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

Summary

CVE	CVE-2021-31916
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-06 17:15:00 UTC
Updated	2022-01-01 17:51:00 UTC
Description	An out-of-bounds (OOB) memory write flaw was found in list_devices in drivers/md/dm-ioctl.c in the Multi-device driver mod

Risk And Classification

Problem Types: CWE-787

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
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
dm ioctl: fix out of bounds array access when no devices · torvalds/linux@4edbe1d · GitHub	MISC	github.com
[SECURITY] [DLA 2689-1] linux security update	MLIST	lists.debian.org
1946965 – (CVE-2021-31916) CVE-2021-31916 kernel: out of bounds array access in drivers/md/dm-ioctl.c	MISC	bugzilla.redhat.com
[SECURITY] [DLA 2690-1] linux-4.19 security update	MLIST	lists.debian.org
oss-sec: Linux Kernel: out of bounds array access in dm-ioctl.c	MISC	seclists.org
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

[159276](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9305)

[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)

[159280](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9308)

[159296](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9346)

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

[178679](#) Debian Security Update for linux-4.19 (DLA 2690-1)

[178680](#) Debian Security Update for linux (DLA 2689-1)

[180153](#) Debian Security Update for linux (CVE-2021-31916)

[198365](#) Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4948-1)

[198398](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4979-1)

[198401](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4982-1)

[198403](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4984-1)

[239816](#) Red Hat Update for kernel security (RHSA-2021:4356)

[239879](#) Red Hat Update for kernel-rt (RHSA-2021:4140)

[352366](#) Amazon Linux Security Advisory for kernel: ALAS-2021-1503

[352831](#) Amazon Linux Security Advisory for kernel: ALAC2012-2021-030

[352832](#) Amazon Linux Security Advisory for kmod-sfc: ALAC2012-2021-031

[352833](#) Amazon Linux Security Advisory for kmod-mlx5: ALAC2012-2021-032

[390223](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0022)

[610372](#) Google Pixel Android October 2021 Security Patch Missing

[610381](#) Google Android November 2021 Security Patch Missing for Huawei EMUI

[670488](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2246)

[670514](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2272)

[670543](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2301)

[670578](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2336)

[670634](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2392)

[671047](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2588)

751399	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1501-1)
751406	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3806-1)
751424	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3848-1)
751436	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3877-1)
751437	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3876-1)
751441	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3876-1)
751451	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3935-1)
751462	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3941-1)
751473	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3969-1)
751476	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3972-1)
900096	CBL-Mariner Linux Security Update for kernel 5.10.52.1
900304	CBL-Mariner Linux Security Update for kernel 5.10.57.1
900319	CBL-Mariner Linux Security Update for kernel 5.10.60.1
901545	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6558-1)
903632	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4193)
905761	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4193-1)
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](#)