



CVE-2021-26931

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

Summary

CVE	CVE-2021-26931
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-17 02:15:00 UTC
Updated	2023-11-07 03:31:00 UTC
Description	An issue was discovered in the Linux kernel 2.6.39 through 5.10.16, as used in Xen. Block, net, and SCSI backends consid

Risk And Classification

Problem Types: CWE-770

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	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

References

Reference	Source	Link	T
XSA-362 - Xen Security Advisories	MISC	xenbits.xen.org	P
[SECURITY] Fedora 33 Update: kernel-5.10.18-200.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] [DLA 2586-1] linux security update	MLIST	lists.debian.org	
[SECURITY] [DLA 2610-1] linux-4.19 security update	MLIST	lists.debian.org	
February 2021 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
[SECURITY] Fedora 32 Update: kernel-5.10.18-100.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	M
[SECURITY] Fedora 32 Update: kernel-5.10.18-100.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: kernel-5.10.18-200.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	M

CVE Program record

CVE.ORG www.cve.org

c

NVD vulnerability detail

NVD nvd.nist.gov

c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159132](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9135)

[159133](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9136)

[174764](#) SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2021:0738-1)

[174768](#) SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2021:0735-1)

[174770](#) SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2021:0741-1)

[174772](#) SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2021:0737-1)

[174774](#) SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2021:0740-1)

[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)

[174950](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 21 for SLE 15) (SUSE-SU-2021:1344-1)

[174954](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 36 for SLE 12 SP3) (SUSE-SU-2021:1373-1)

[174955](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 17 for SLE 15 SP1) (SUSE-SU-2021:1365-1)

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

[179857](#) Debian Security Update for linux (CVE-2021-26931)

[198323](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4904-1)

[198325](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4909-1)

[198366](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4949-1)

[198371](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4946-1)

[352244](#) Amazon Linux Security Advisory for kernel: ALAS-2021-1487

[352254](#) Amazon Linux Security Advisory for kernel: ALAS2-2021-1616

[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

379053 Citrix XenServer Security Updates (CTX296603)
6140382 AWS Bottlerocket Security Update for kernel (GHSA-g55q-88v2-6r3m)
671804 EulerOS Security Update for kernel (EulerOS-SA-2022-1844)
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)
750324 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0393-1)
900098 CBL-Mariner Linux Security Update for kernel 5.4.91
903482 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3896)
906082 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3896-1)

© [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](#)