



CVE-2021-29650

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

Summary

CVE	CVE-2021-29650
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-30 21:15:00 UTC
Updated	2023-11-07 03:32:00 UTC
Description	An issue was discovered in the Linux kernel before 5.11.11. The netfilter subsystem allows attackers to cause a denial of se

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	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 32 Update: kernel-5.11.11-100.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 2689-1] linux security update	MLIST	lists.debian.org
[SECURITY] Fedora 34 Update: kernel-headers-5.11.11-300.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 33 Update: kernel-5.11.11-200.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 32 Update: kernel-5.11.11-100.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 34 Update: kernel-headers-5.11.11-300.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 2690-1] linux-4.19 security update	MLIST	lists.debian.org
[SECURITY] Fedora 33 Update: kernel-5.11.11-200.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.11.11	MISC	cdn.kernel.org

kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.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

159175 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9215)
159177 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9220)
159178 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9221)
159179 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9222)
159180 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9223)
159375 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-3327)
159492 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)
174996 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:14724-1)
174997 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1571-1)
178679 Debian Security Update for linux-4.19 (DLA 2690-1)
178680 Debian Security Update for linux (DLA 2689-1)
180216 Debian Security Update for linux (CVE-2021-29650)
198363 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4945-1)
198364 Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4947-1)
198365 Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4948-1)
198366 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4949-1)
198371 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4946-1)
198377 Ubuntu Security Notification for Linux kernel (Raspberry Pi) vulnerabilities (USN-4945-2)
239602 Red Hat Update for kernel-rt (RHSA-2021:3328)
239603 Red Hat Update for kernel (RHSA-2021:3327)
239816 Red Hat Update for kernel security (RHSA-2021:4356)
239879 Red Hat Update for kernel-rt (RHSA-2021:4140)
257109 CentOS Security Update for kernel (CESA-2021:3327)

281064 Fedora Security Update for kernel, kernel-headers (FEDORA-2021-2306e89112)
281065 Fedora Security Update for kernel, kernel-headers (FEDORA-2021-6b0f287b8b)
281395 Fedora Security Update for kernel (FEDORA-2021-41fb54ae9f)
281396 Fedora Security Update for kernel (FEDORA-2021-2306e89112)
281397 Fedora Security Update for kernel (FEDORA-2021-6b0f287b8b)
352475 Amazon Linux Security Advisory for kernel: ALAS-2021-1516
352489 Amazon Linux Security Advisory for kernel: ALAS2-2021-1685
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
353149 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-002
390225 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0016)
6140101 AWS Bottlerocket Security Update for kernel (GHSA-74hg-j92w-jg2f)
670438 EulerOS Security Update for kernel (EulerOS-SA-2021-2062)
670449 EulerOS Security Update for kernel (EulerOS-SA-2021-2051)
671268 EulerOS Security Update for kernel (EulerOS-SA-2022-1196)
671344 EulerOS Security Update for kernel (EulerOS-SA-2022-1271)
750001 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1572-1)
750003 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1574-1)
750004 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1573-1)
750005 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1595-1)
750006 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1596-1)
750012 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1622-1)
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)
750137 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1915-1)
750216 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0716-1)
750643 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0873-1)

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)
754120 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2611-1)
754145 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2651-1)
900100 CBL-Mariner Linux Security Update for kernel 5.10.52.1
900305 CBL-Mariner Linux Security Update for kernel 5.10.57.1
900320 CBL-Mariner Linux Security Update for kernel 5.10.60.1
901912 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6553-1)
903301 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4038)
906173 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4038-1)
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](#)