



CVE-2021-33033

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

Summary

CVE	CVE-2021-33033
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-14 23:15:00 UTC
Updated	2021-06-09 18:37:00 UTC
Description	The Linux kernel before 5.11.14 has a use-after-free in cipso_v4_genopt in net/ipv4/cipso_ipv4.c because the CIPSO and C

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
KASAN: use-after-free Read in cipso_v4_genopt	MISC	syzkaller.appspot.com	
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.11.14	MISC	cdn.kernel.org	
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.11.7	MISC	cdn.kernel.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
SyzScope - KASAN: use-after-free Read in cipso_v4_genopt	MISC	sites.google.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159304 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9349)

159305 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9351)
159306 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9362)
159307 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9363)
159310 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-2725)
179118 Debian Security Update for linux (DLA 2940-1)
180016 Debian Security Update for linux (CVE-2021-33033)
198398 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4979-1)
198403 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4984-1)
239523 Red Hat Update for kernel-rt (RHSA-2021:2726)
239524 Red Hat Update for kernel (RHSA-2021:2725)
239879 Red Hat Update for kernel-rt (RHSA-2021:4140)
257100 CentOS Security Update for kernel (CESA-2021:2725)
352366 Amazon Linux Security Advisory for kernel: ALAS-2021-1503
353242 Amazon Linux Security Advisory for kernel : ALAC2012-2022-036
353243 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2022-037
353244 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2022-038
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)
751336 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1460-1)
751342 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3641-1)
751346 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3655-1)
751349 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1477-1)
751353 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3675-1)
751381 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3748-1)
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)
751473	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3969-1)
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
901876	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6561-1)
902912	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4203)
906180	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4203-1)
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](#)