



CVE-2021-45485

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

Summary

CVE	CVE-2021-45485
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-25 02:15:00 UTC
Updated	2023-02-24 15:07:00 UTC
Description	In the IPv6 implementation in the Linux kernel before 5.13.3, net/ipv6/output_core.c has an information leak because of cer

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	Aff A400	-	All	All	All
Operating System	Netapp	Aff A400 Firmware	-	All	All	All
Hardware	Netapp	All Flash Fabric-attached Storage 8300	-	All	All	All
Operating System	Netapp	All Flash Fabric-attached Storage 8300 Firmware	-	All	All	All
Hardware	Netapp	All Flash Fabric-attached Storage 8700	-	All	All	All
Operating System	Netapp	All Flash Fabric-attached Storage 8700 Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H300e	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H300s	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410c	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410s	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H500e	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H500s	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H610c	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H610s	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H615c	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H700e	-	All	All	All

Hardware	Netapp	Baseboard Management Controller H700s	-	All	All	All
Operating System	Netapp	Brocade Fabric Operating System Firmware	-	All	All	All
Application	Netapp	E-series Santricity Os Controller	-	All	All	All
Hardware	Netapp	Fabric-attached Storage 8300	-	All	All	All
Operating System	Netapp	Fabric-attached Storage 8300 Firmware	-	All	All	All
Hardware	Netapp	Fabric-attached Storage 8700	-	All	All	All
Operating System	Netapp	Fabric-attached Storage 8700 Firmware	-	All	All	All
Hardware	Netapp	Fabric-attached Storage A400	-	All	All	All
Operating System	Netapp	Fabric-attached Storage A400 Firmware	-	All	All	All
Application	Netapp	Fas/aff Baseboard Management Controller 8300	-	All	All	All
Application	Netapp	Fas/aff Baseboard Management Controller 8700	-	All	All	All
Application	Netapp	Fas/aff Baseboard Management Controller A400	-	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H610c	-	All	All	All
Operating System	Netapp	H610c Firmware	-	All	All	All
Hardware	Netapp	H610s	-	All	All	All
Operating System	Netapp	H610s Firmware	-	All	All	All
Hardware	Netapp	H615c	-	All	All	All
Operating System	Netapp	H615c Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All

Hardware	Netapp	Hci Compute Node	-	All	All	All
Operating System	Netapp	Hci Compute Node Firmware	-	All	All	All
Application	Netapp	Solidfire Enterprise Sds Hci Storage Node	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Application	Oracle	Communications Cloud Native Core Binding Support Function	22.1.3	All	All	All
Application	Oracle	Communications Cloud Native Core Network Exposure Function	22.1.1	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	22.2.0	All	All	All

References

Reference	Source	Link	Tags
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.3	MISC	cdn.kernel.org	
arxiv.org/pdf/2112.09604.pdf	MISC	arxiv.org	
CVE-2021-45485 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159825 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-1988)
180442 Debian Security Update for linux (CVE-2021-45485)
240275 Red Hat Update for kernel-rt (RHSA-2022:1975)
240298 Red Hat Update for kernel security (RHSA-2022:1988)
240734 Red Hat Update for kernel-rt (RHSA-2022:6991)
240738 Red Hat Update for kernel security (RHSA-2022:6983)
671401 EulerOS Security Update for kernel (EulerOS-SA-2022-1328)
671441 EulerOS Security Update for kernel (EulerOS-SA-2022-1366)
671448 EulerOS Security Update for kernel (EulerOS-SA-2022-1450)
671474 EulerOS Security Update for kernel (EulerOS-SA-2022-1429)
671535 EulerOS Security Update for kernel (EulerOS-SA-2022-1508)
671703 EulerOS Security Update for kernel (EulerOS-SA-2022-1735)

751590 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0056-1)
751600 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0068-1)
751602 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0080-1)
751622 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0131-1)
751654 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0197-1)
751657 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0198-1)
751666 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0169-1)
751698 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0362-1)
751989 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0131-1)
751993 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0198-1)
753264 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0079-1)
753267 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0169-1)
753355 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0056-1)
753462 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0289-1)
900504 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (7102)
900981 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (7109-1)
905747 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (7102-1)
940517 AlmaLinux Security Update for kernel (ALSA-2022:1988)

© [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](#)