CVE-2022-27666

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-27666
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-23 06:15:00 UTC
Updated	2023-02-01 14:32:00 UTC
Description	A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw a

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	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.17	-	All	All
Operating System	Linux	Linux Kernel	5.17	rc1	All	All
Operating System	Linux	Linux Kernel	5.17	rc2	All	All
Operating System	Linux	Linux Kernel	5.17	rc3	All	All
Operating System	Linux	Linux Kernel	5.17	rc4	All	All
Operating System	Linux	Linux Kernel	5.17	rc5	All	All
Operating System	Linux	Linux Kernel	5.17	rc6	All	All
Operating System	Linux	Linux Kernel	5.17	rc7	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	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
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-5127-1 linux	DEBIAN	www.debian.org
Debian -- Security Information -- DSA-5173-1 linux	DEBIAN	www.debian.org
esp: Fix possible buffer overflow in ESP transformation · torvalds/linux@ebe48d3 · GitHub	MISC	github.com
March 2022 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.16.15	MISC	cdn.kernel.org
2061633 – (CVE-2022-0886) CVE-2022-0886 kernel: buffer overflow in IPsec ESP transformation code	MISC	bugzilla.redhat.com
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

159785 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9368)

159786 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9366)

159787 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9367)

159788 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9365)

159931 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5249)

159962 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5316)

179258 Debian Security Update for linux (DSA 5127-1)

180605 Debian Security Update for linux (DSA 5173-1)

182989 Debian Security Update for linux (CVE-2022-27666)

198716 Ubuntu Security Notification for Linux kernel (OEM) Vulnerability (USN-5353-1)

198721 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5358-1)

198722 Ubuntu Security Notification for Linux kernel Vulnerability (USN-5357-1)

198726 Ubuntu Security Notification for Linux kernel Vulnerability (USN-5357-2)

198727 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5358-2)

198731 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5368-1)

198740 Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-5377-1)

240383 Red Hat Update for kpatch-patch (RHSA-2022:4809)

240390 Red Hat Update for kernel-rt (RHSA-2022:4835)

240392 Red Hat Update for kernel security (RHSA-2022:4829)

240487 Red Hat Update for kpatch-patch (RHSA-2022:5214)

240494 Red Hat Update for kernel (RHSA-2022:5220)

240495 Red Hat Update for kpatch-patch (RHSA-2022:5219)

240499 Red Hat Update for kernel (RHSA-2022:5249)

240524 Red Hat Update for kpatch-patch (RHSA-2022:5476)

240527 Red Hat Update for kernel-rt (RHSA-2022:5267)

240528 Red Hat Update for kernel-rt (RHSA-2022:5344)

240531 Red Hat Update for kernel-rt (RHSA-2022:5224)

240534 Red Hat Update for kernel (RHSA-2022:5316)

353215 Amazon Linux Security Advisory for kernel : ALAS-2022-1581

353216 Amazon Linux Security Advisory for kernel : ALAS2-2022-1774

353237 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-025

353238 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-013

376925 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125)

377124 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0029)

377181 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2022:0022)

610430 Google Android September 2022 Security Patch Missing for Huawei EMUI

610432 Google Pixel Android August 2022 Security Patch Missing

6140115 AWS Bottlerocket Security Update for kernel (GHSA-mfvh-3cwr-cg4c)

671734 EulerOS Security Update for kernel (EulerOS-SA-2022-1791)

671749 EulerOS Security Update for kernel (EulerOS-SA-2022-1808)

671804 EulerOS Security Update for kernel (EulerOS-SA-2022-1844)

671817 EulerOS Security Update for kernel (EulerOS-SA-2022-1868)

671870 EulerOS Security Update for kernel (EulerOS-SA-2022-1934)

752036 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1183-1)

752039 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1196-1)

752042 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1197-1)

752048 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1266-1)

752053 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1267-1)

753103 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 16 for SLE 15 SP3) (SUSE-SU-2022:1224-1)

753173 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 4 for SLE 15 SP3) (SUSE-SU-2022:1246-1)

753193 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15) (SUSE-SU-2022:1230-1)

753265 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 27 for SLE 15) (SUSE-SU-2022:1261-1)

753340 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 12 for SLE 15 SP3) (SUSE-SU-2022:1223-1)

753344 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 27 for SLE 15 SP1) (SUSE-SU-2022:1172-1)

753351 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 15 for SLE 15 SP3) (SUSE-SU-2022:1269-1)

753373 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1257-1)

753392 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15 SP1) (SUSE-SU-2022:1212-1)

753417 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1163-1)

753418 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 28 for SLE 12 SP5) (SUSE-SU-2022:1215-1)

753427 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1407-1)

753430 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15 SP1) (SUSE-SU-2022:1193-1)

753442 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 18 for SLE 15 SP2) (SUSE-SU-2022:1194-1)

753447 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 25 for SLE 15) (SUSE-SU-2022:1248-1)

900775 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9110)

901358 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9110-1)

901808 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9120-1)

905390 Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (13222)

905391 Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (13228)

905522 Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (13228-1)

905811 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9110-2)

905891 Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (13222-2)

906264 Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (13228-2)

906303 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9120-2)

906576 Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (13222-4)

940589 AlmaLinux Security Update for kernel-rt (ALSA-2022:5344)

940593 AlmaLinux Security Update for kernel (ALSA-2022:5316)

940618 AlmaLinux Security Update for kernel (ALSA-2022:5249)

940638 AlmaLinux Security Update for kernel-rt (ALSA-2022:5267)

960258 Rocky Linux Security Update for kernel-rt (RLSA-2022:5344)

960418 Rocky Linux Security Update for kernel (RLSA-2022:5316)