CVE-2022-3629

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-3629
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-21 06:15:00 UTC
Updated	2023-11-07 03:51:00 UTC
Description	A vulnerability was found in Linux Kernel. It has been declared as problematic. This vulnerability affects the function vsock_

Risk And Classification

Problem Types: CWE-401

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	Linux	Linux Kernel	-	All	All	All

References

Reference	Source	Link	Tags
CVE-2022-3629 | Linux Kernel af_vsock.c vsock_connect memory leak (DLA 3173-1)	MISC	vuldb.com	
CVE-2022-3629 | Linux Kernel IPsec af_vsock.c vsock_connect memory leak	N/A	vuldb.com	
[SECURITY] [DLA 3173-1] linux-5.10 security update	MLIST	lists.debian.org	
kernel/git/klassert/ipsec-next.git - Steffen Klassert's ipsec-next networking tree	N/A	git.kernel.org	
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

160345 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-10065)

181153 Debian Security Update for linux (CVE-2022-3629)

181190 Debian Security Update for linux-5.10 (DLA 3173-1)

377891 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0002)

378043 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0011)

390269 Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0031)

672495 EulerOS Security Update for kernel (EulerOS-SA-2023-1012)

672516 EulerOS Security Update for kernel (EulerOS-SA-2023-1037)

672532 EulerOS Security Update for kernel (EulerOS-SA-2023-1126)

672564 EulerOS Security Update for kernel (EulerOS-SA-2023-1102)

672582 EulerOS Security Update for kernel (EulerOS-SA-2023-1345)

672653 EulerOS Security Update for kernel (EulerOS-SA-2023-1388)

672668 EulerOS Security Update for kernel (EulerOS-SA-2023-1360)

672711 EulerOS Security Update for kernel (EulerOS-SA-2023-1507)

752813 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3930-1)

752839 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3929-1)

752880 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4053-1)

752889 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3897-1)

752911 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3998-1)

752913 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4072-1)

752944 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4273-1)

752959 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4272-1)

753038 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4573-1)

753039 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4574-1)

753051 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4589-1)

753060 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4615-1)

753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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