CVE-2022-3643

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-3643
State	PUBLIC
Assigner	security@xen.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-07 01:15:00 UTC
Updated	2023-11-29 15:15:00 UTC
Description	Guests can trigger NIC interface reset/abort/crash via netback It is possible for a guest to trigger a NIC interface reset/abort

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Broadcom	Bcm5780	-	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source
[SECURITY] [DLA 3245-1] linux security update	MLIST
Kernel Live Patch Security Notice LSN-0099-1 ≈ Packet Storm	
oss-security - Xen Security Advisory 423 v2 (CVE-2022-3643) - Guests can trigger NIC interface reset/abort/crash via netback	MLIST
[SECURITY] [DLA 3244-1] linux-5.10 security update	MLIST
xenbits.xenproject.org/xsa/advisory-423.txt	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181438 Debian Security Update for linux (CVE-2022-3643)

181440 Debian Security Update for linux-5.10 (DLA 3244-1)

181565 Debian Security Update for linux (DLA 3245-1)

199103 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5803-1)

199105 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5804-1)

199106 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5804-2)

199111 Ubuntu Security Notification for Linux kernel (IBM) Vulnerabilities (USN-5808-1)

199118 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5814-1)

199121 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5813-1)

199132 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5829-1)

199136 Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-5831-1)

199137 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5830-1)

199138 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5832-1)

199160 Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5860-1)

199165 Ubuntu Security Notification for Linux kernel (Dell300x) Vulnerabilities (USN-5861-1)

199179 Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5877-1)

199180 Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5875-1)

199183 Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-5879-1)

199213 Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-5918-1)

199490 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5802-1)

199519 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5863-1)

199547 Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-5794-1)

354668 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-025

354669 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-012

354670 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-041

354736 Amazon Linux Security Advisory for kernel : ALAS2-2023-1932

354842 Amazon Linux Security Advisory for kernel : ALAS-2023-1706

355199 Amazon Linux Security Advisory for kernel : ALAS2023-2023-070

378468 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)

378468 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)

378512 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)

379435 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2024:0012)

6140027 AWS Bottlerocket Security Update for kernel (GHSA-qqmh-8q8r-6p7p)

6140061 AWS Bottlerocket Security Update for kernel (GHSA-qqmh-8q8r-6p7p)

753014 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4505-1)

753020 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4585-1)

753034 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4504-1)

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)

753047 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4566-1)

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)

753562 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0134-1)

753583 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0152-1)

753688 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0406-1)

904975 Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.79.1-1.cm2 (12545)

904995 Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.80.1-1.cm2 (12550)

905010 Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.81.1-1.cm2 (12552)

905045 Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.74.1-1.cm2 (12538)

905047 Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.72.1-1.cm2 (12533)

905082 Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.48.1-4.cm2 (12521)

905134 Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.82.1-1.cm2 (12556)

905147 Common Base Linux Mariner (CBL-Mariner) Security Update for livepatch-5.15.77.1-1.cm2 (12539)

CVE.report and Source URL Uptime Status status.cve.report