CVE-2021-29657

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-29657
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-22 17:15:00 UTC
Updated	2023-05-19 16:51:00 UTC
Description	arch/x86/kvm/svm/nested.c in the Linux kernel before 5.11.12 has a use-after-free in which an AMD KVM guest can bypass

Risk And Classification

Problem Types: CWE-416 | CWE-367

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	CONFIRM	git.kernel.org	
2177 - project-zero - Project Zero - Monorail	MISC	bugs.chromium.org	
KVM nested_svm_vmrun Double Fetch ≈ Packet Storm	MISC	packetstormsecurity.com	
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.11.12	CONFIRM	cdn.kernel.org	
CVE-2021-29657 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180529 Debian Security Update for linux (CVE-2021-29657)

198365 Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4948-1)

900292 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

901480 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6554-1)

902864 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5046)

905925 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5046-1)