CVE-2022-1263

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-1263
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-31 16:15:00 UTC
Updated	2022-09-07 13:11:00 UTC
Description	A NULL pointer dereference issue was found in KVM when releasing a vCPU with dirty ring support enabled. This flaw allov

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.18	rc1	All	All
Operating System	Linux	Linux Kernel	5.18	rc2	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Sourc
KVM: avoid NULL pointer dereference in kvm_dirty_ring_push · torvalds/linux@5593473 · GitHub	MISC
2072698 – (CVE-2022-1263) CVE-2022-1263 kernel: KVM: NULL pointer dereference in kvm_dirty_ring_push in virt/kvm/dirty_ring.c	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
oss-security - Linux kernel: x86/kvm: null-ptr-deref in kvm_dirty_ring_push	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184079	Debian Security Update for linux (CVE-2022-1263)
198822	Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5469-1)
353964	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-001
354327	Amazon Linux Security Advisory for kernel : ALAS2022-2022-083
354468	Amazon Linux Security Advisory for kernel : ALAS2022-2022-185
354542	Amazon Linux Security Advisory for kernel : ALAS-2022-185
355199	Amazon Linux Security Advisory for kernel : ALAS2023-2023-070
355565	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-023
752750	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3844-1)
753063	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
753095	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3585-1)
903753	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10812)
903857	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10820)
904099	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10812-1)
904165	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10820-1)
905855	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10812-2)
906513	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10820-2)