CVE-2021-20257

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-20257
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-16 15:15:00 UTC
Updated	2023-02-12 22:15:00 UTC
Description	An infinite loop flaw was found in the e1000 NIC emulator of the QEMU. This issue occurs while processing transmits (tx) d

Risk And Classification

Problem Types: CWE-835

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	Fedoraproject	Fedora	33	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Redhat	Codeready Linux Builder	-	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All	All	All
Application	Redhat	Openstack Platform	10.0	All	All	All
Application	Redhat	Openstack Platform	13.0	All	All	All

References

Reference	Source	Link

Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.
March 2022 QEMU Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security
e1000: fail early for evil descriptor · qemu/qemu@3de46e6 · GitHub	MISC	github.c
oss-security - CVE-2021-20257 QEMU: net: e1000: infinite loop while processing transmit descriptors	MISC	www.op
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists.deb
1930087 – (CVE-2021-20257) CVE-2021-20257 QEMU: net: e1000: infinite loop while processing transmit descriptors	MISC	bugzilla
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	security
[PATCH] e1000: fail early for evil descriptor	MISC	lists.gnu
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159294 Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9335)
- 159566 Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2021-9568)
- 159578 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2021-5238)
- 159582 Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9638)
- 159672 Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2022-9172)
- 174875 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:1023-1)
- 174920 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1243-1)
- 174921 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1245-1)
- 174922 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1240-1)
- 174923 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1241-1)
- 174924 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1244-1)
- 174926 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1242-1)
- 174928 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:1252-1)
- 174929 SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:1251-1)
- 178540 Debian Security Update for qemu (DLA 2623-1)
- 179701 Debian Security Update for qemu (CVE-2021-20257)

180995 Debian Security Update for qemu (DLA 3099-1)

198432 Ubuntu Security Notification for QEMU vulnerabilities (USN-5010-1)

239978 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:5238)

355321 Amazon Linux Security Advisory for qemu : ALAS2-2023-2060

377413 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)

502168 Alpine Linux Security Update for qemu

710604 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)

750097 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1837-1)

750120 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1893-1)

750124 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1894-1)

750129 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1895-1)

750138 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1918-1)

750152 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1947-1)

750251 OpenSUSE Security Update for qemu (openSUSE-SU-2021:0600-1)

750827 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1043-1)

900764 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9056)

901546 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9068)

902039 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (9056-1)

902098 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu (9068-1)

940065 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:5238)

960270 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:5238)