CVE-2020-16092

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-16092
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-11 16:15:00 UTC
Updated	2022-09-30 12:49:00 UTC
Description	In QEMU through 5.0.0, an assertion failure can occur in the network packet processing. This issue affects the e1000e and

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	L
oss-security - CVE-2020-16092 QEMU: reachable assertion failure in net_tx_pkt_add_raw_fragment() in hw/net/net_tx_pkt.c	MISC	w
[PATCH 0/2] assertion failure in net_tx_pkt_add_raw_fragment() in hw/net	MISC	lis
[security-announce] openSUSE-SU-2020:1664-1: important: Security update	SUSE	lis
CVE-2020-16092 QEMU Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	s
Debian -- Security Information -- DSA-4760-1 qemu	DEBIAN	w
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	s
USN-4467-1: QEMU vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	u

[SECURITY] [DLA 2373-1] qemu security update	MLIST	li
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159456 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2021-1762)
- 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)
- 239166 Red Hat Update for qemu-kvm-rhev (RHSA-2021:0934)
- 239306 Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:1762)
- 352242 Amazon Linux Security Advisory for qemu-kvm: ALAS-2021-1488
- 352251 Amazon Linux Security Advisory for qemu: ALAS2-2021-1617
- 377247 Alibaba Cloud Linux Security Update for qemu-kvm-ma (ALINUX2-SA-2021:0007)
- 377413 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)
- 377426 Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2021:0008)
- 502352 Alpine Linux Security Update for qemu
- 710604 Gentoo Linux QEMU Multiple Vulnerabilities (GLSA 202208-27)
- 900050 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
- 903498 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1950)
- 940118 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:1762)
- 960265 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:1762)

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