CVE-2020-11102

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-11102
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-06 16:15:00 UTC
Updated	2020-05-13 01:15:00 UTC
Description	hw/net/tulip.c in QEMU 4.2.0 has a buffer overflow during the copying of tx/rx buffers because the frame size is not validate

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	4.2.0	All	All	All
Application	Qemu	Qemu	4.2.0	All	All	All

References

Reference	Source	Link	Tags
QEMU: Multiple vulnerabilities (GLSA 202005-02) — Gentoo security	GENTOO	security.gentoo.org	
[PULL 12/13] net: tulip: check frame size and r/w data length	MISC	lists.gnu.org	Mailing List, Third Pa
oss-security - CVE-2020-11102 QEMU: tulip: OOB access in tulip_copy_tx_buffers	MLIST	www.openwall.com	Mailing List, Third Pa
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

900050 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0

903667 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1968)