CVE-2020-15863

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-15863
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-28 16:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	hw/net/xgmac.c in the XGMAC Ethernet controller in QEMU before 07-20-2020 has a buffer overflow. This occurs during pa

Risk And Classification

Problem Types: CWE-787

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	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	10.0	All	All	All
Application	Qemu	Qemu	5.1.0	rc0	All	All
Application	Qemu	Qemu	5.1.0	rc0	All	All
Application	Qemu	Qemu	All	All	All	All

References

Reference	Source	Link	T
git.qemu.org Git - qemu.git/commitdiff		git.qemu.org	
[PATCH] hw/net/xgmac: Fix buffer overflow in xgmac_enet_send()	MISC	lists.nongnu.org	M
[security-announce] openSUSE-SU-2020:1664-1: important: Security update	SUSE	lists.opensuse.org	T

git.qemu.org Git - qemu.git/commitdiff	CONFIRM	git.qemu.org	F
Debian -- Security Information -- DSA-4760-1 qemu	DEBIAN	www.debian.org	T
oss-security - CVE-2020-15863 QEMU: stack-based overflow in xgmac_enet_send() in hw/net/xgmac.c	CONFIRM	www.openwall.com	M
QEMU: Multiple Vulnerabilities (GLSA 202208-27) — Gentoo security	GENTOO	security.gentoo.org	
USN-4467-1: QEMU vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	T
Re: [PATCH] hw/net/xgmac: Fix buffer overflow in xgmac_enet_send()	MISC	lists.nongnu.org	M
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 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)
- 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
- 903671 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1960)