CVE-2020-25084

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25084
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-25 05:15:00 UTC
Updated	2022-09-23 15:28:00 UTC
Description	QEMU 5.0.0 has a use-after-free in hw/usb/hcd-xhci.c because the usb_packet_map return value is not checked.

Risk And Classification

Problem Types: CWE-416

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	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Qemu	Qemu	5.0.0	-	All	All
Application	Qemu	Qemu	5.0.0	-	All	All

References

Reference	Source	Link	Tags
oss-security - CVE-2020-25084 QEMU: usb: use-after-free issue while setting up packet	CONFIRM	www.openwall.com	Mailing List, Pa
[PULL 01/18] hw: xhci: check return value of 'usb_packet_map'	MISC	lists.nongnu.org	Mailing List, Pa
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists.debian.org	
[SECURITY] [DLA 2560-1] qemu security update	MLIST	lists.debian.org	Mailing List, Th
October 2020 QEMU Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Third Party Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 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)
- 180995 Debian Security Update for qemu (DLA 3099-1)
- 502352 Alpine Linux Security Update for qemu
- 750251 OpenSUSE Security Update for qemu (openSUSE-SU-2021:0600-1)