CVE-2020-25741

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25741
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-02 09:15:00 UTC
Updated	2020-10-14 14:27:00 UTC
Description	fdctrl_write_data in hw/block/fdc.c in QEMU 5.0.0 has a NULL pointer dereference via a NULL block pointer for the current

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	5.0.0	-	All	All
Application	Qemu	Qemu	5.0.0	-	All	All

References

Reference	Source	Link	Tags
Re: [PATCH] fdc: check null block pointer before blk_pwrite	MISC	lists.nongnu.org	Mailing List, F
oss-security - QEMU: NULL pointer derefrence issues	CONFIRM	www.openwall.com	Mailing List, T
sciebo	MISC	ruhr-uni-bochum.sciebo.de	Third Party A
October 2020 QEMU Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

502352 Alpine Linux Security Update for qemu