CVE-2020-25085

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-25085
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 16:06:00 UTC
Description	QEMU 5.0.0 has a heap-based Buffer Overflow in flatview_read_continue in exec.c because hw/sd/sdhci.c mishandles a w

Risk And Classification

Problem Types: CWE-787

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
oss-security - CVE-2021-3409 QEMU: sdhci: incomplete fix for CVE-2020-17380/CVE-2020-25085	MLIST	www.openwall.com
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists.debian.org
[SECURITY] [DLA 2469-1] qemu security update	MLIST	lists.debian.org
Re: [PATCH v2 3/3] hw/sd/sdhci: Fix DMA Transfer Block Size field	MISC	lists.nongnu.org
October 2020 QEMU Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
Bug #1892960 “Heap-overflow in flatview_read through sdhci_data_...” : Bugs : QEMU	MISC	bugs.launchpad.net
oss-security - CVE-2020-25085 QEMU: sdhci: out-of-bounds access issue while doing multi block SDMA	CONFIRM	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 178540 Debian Security Update for qemu (DLA 2623-1)
- 180995 Debian Security Update for qemu (DLA 3099-1)
- 502352 Alpine Linux Security Update for qemu
- 671198 EulerOS Security Update for qemu (EulerOS-SA-2022-1034)
- 671203 EulerOS Security Update for qemu (EulerOS-SA-2022-1014)
- 750097 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1837-1)
- 750120 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1893-1)
- 750149 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1942-1)
- 750771 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1942-1)
- 750827 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1043-1)
- 750910 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:2591-1)
- 750912 OpenSUSE Security Update for qemu (openSUSE-SU-2021:2591-1)
- 752675 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3594-1)
- 752725 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2022:3768-1)
- 753802 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0761-1)