



CVE-2020-17380

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-17380 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-01-30 06:15:00 UTC |
| Updated | 2022-10-14 03:48:00 UTC |
| Description | A heap-based buffer overflow was found in QEMU through 5.0.0 in the SDHCI device emulation support. It could occur whil |

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 | 9.0 | All | All | All |
| Application | Qemu | Qemu | All | All | All | All |

References

| Reference | Source |
|---|--------|
| 1862167 – (CVE-2020-17380) CVE-2020-17380 QEMU: heap buffer overflow in sdhci_sdma_transfer_multi_blocks() in hw/sd/sdhci.c | CONI |
| oss-security - CVE-2021-3409 QEMU: sdhci: incomplete fix for CVE-2020-17380/CVE-2020-25085 | MLIS |
| [PATCH v1] sd: sdhci: assert data_count is within fifo_buffer | CONI |
| [SECURITY] [DLA 2623-1] qemu security update | MLIS |
| CVE-2020-17380 QEMU Vulnerability in NetApp Products NetApp Product Security | CONI |
| CVE Program record | CVE. |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178540](#) Debian Security Update for qemu (DLA 2623-1)

| |
|--|
| 181630 Debian Security Update for qemu (DLA 3362-1) |
| 502352 Alpine Linux Security Update for qemu |
| 750149 SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1942-1) |
| 750771 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1942-1) |
| 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) |
| 900209 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0 |
| 903656 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (3856) |

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)