



# CVE-2020-13253

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-13253
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-05-27 15:15:00 UTC
<b>Updated</b>	2022-09-23 15:29:00 UTC
<b>Description</b>	sd_wp_addr in hw/sd/sd.c in QEMU 4.2.0 uses an unvalidated address, which leads to an out-of-bounds read during sdhci_

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Qemu</a>	<a href="#">Qemu</a>	All	All	All	All

## References

Reference	Source	Link
[PATCH 1/2] sd: check bit number before setting card_status flag	MISC	<a href="#">lists.gnu.org</a>
1838546 – (CVE-2020-13253) CVE-2020-13253 QEMU: sd: OOB access could crash the guest resulting in DoS	CONFIRM	<a href="#">bugzilla.redhat.com</a>
[SECURITY] [DLA 3099-1] qemu security update	MLIST	<a href="#">lists.debian.org</a>
QEMU: Multiple vulnerabilities (GLSA 202011-09) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>

USN-4467-1: QEMU vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.cc</a>
oss-security - CVE-2020-13253 QEMU: sd: OOB access could crash the guest resulting in DoS	CONFIRM	<a href="https://www.openwall.com/lists/oss-security">www.openwa</a>
[SECURITY] [DLA 2373-1] qemu security update	MLIST	<a href="https://lists.debian.org">lists.debian.or</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">180995</a> Debian Security Update for qemu (DLA 3099-1)
<a href="#">751671</a> OpenSUSE Security Update for qemu (openSUSE-SU-2022:0210-1)
<a href="#">751742</a> OpenSUSE Security Update for qemu (openSUSE-SU-2022:0210-2)
<a href="#">753802</a> SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2023:0761-1)
<a href="#">900187</a> CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
<a href="#">903305</a> Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (1966)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)