CVE-2020-13253

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-13253
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-27 15:15:00 UTC
Updated	2022-09-23 15:29:00 UTC
Description	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	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
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	All	All	All	All

References

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

USN-4467-1: QEMU vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.co
oss-security - CVE-2020-13253 QEMU: sd: OOB access could crash the guest resulting in DoS	CONFIRM	www.openwa
[SECURITY] [DLA 2373-1] qemu security update	MLIST	lists.debian.or
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

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