# CVE-2020-7039

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-7039 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-01-16 23:15:00 UTC |
| **Updated** | 2021-02-14 03:50:00 UTC |
| **Description** | tcp_emu in tcp_subr.c in libslirp 4.1.0, as used in QEMU 4.2.0, mismanages memory, as demonstrated by IRC DCC comma |

## 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 | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Libslirp Project | Libslirp | 4.1.0 | All | All | All |
| Application | Libslirp Project | Libslirp | 4.1.0 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Application | Qemu | Qemu | 4.2.0 | All | All | All |
| Application | Qemu | Qemu | 4.2.0 | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| slirp: use correct size while emulating IRC commands (ce131029) · Commits · slirp / libslirp · GitLab | MISC | gitlab.freedesktop. |
| Red Hat Customer Portal | REDHAT | access.redhat.com |
| QEMU: Multiple vulnerabilities (GLSA 202005-02) — Gentoo security | GENTOO | security.gentoo.org |
| Bugtraq: [SECURITY] [DSA 4616-1] qemu security update | BUGTRAQ | seclists.org |

| | | |
|---|---|---|
| [SECURITY] [DLA 2076-1] slirp security update | MLIST | lists.debian.org |
| USN-4283-1: QEMU vulnerabilities \| Ubuntu security notices \| Ubuntu | UBUNTU | usn.ubuntu.com |
| Red Hat Customer Portal | REDHAT | access.redhat.com |
| [SECURITY] [DLA 2551-1] slirp security update | MLIST | lists.debian.org |
| tcp_emu: Fix oob access (2655fffe) · Commits · slirp / libslirp · GitLab | MISC | gitlab.freedesktop. |
| oss-security - CVE-2020-7039 QEMU: slirp: OOB buffer access while emulating tcp protocols in tcp_emu() | CONFIRM | www.openwall.com |
| Debian -- Security Information -- DSA-4616-1 qemu | DEBIAN | www.debian.org |
| [SECURITY] [DLA 2090-1] qemu security update | MLIST | lists.debian.org |
| slirp: use correct size while emulating commands (82ebe9c3) · Commits · slirp / libslirp · GitLab | MISC | gitlab.freedesktop. |
| [security-announce] openSUSE-SU-2020:0468-1: important: Security update | SUSE | lists.opensuse.org |
| 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

- 377167 Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2020:0072)
- 377335 Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2022:0110)
- 377413 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)
- 900050 CBL-Mariner Linux Security Update for qemu-kvm 4.2.0
- 903446 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (3579)
- 906000 Common Base Linux Mariner (CBL-Mariner) Security Update for qemu-kvm (3579-1)
- 940144 AlmaLinux Security Update for virt:rhel (ALSA-2020:1358)
- 940554 AlmaLinux Security Update for container-tools:1.0 (ALSA-2020:1360)
- 940555 AlmaLinux Security Update for container-tools:rhel8 (ALSA-2020:0348)
- 960718 Rocky Linux Security Update for virt:rhel (RLSA-2020:1358)
- 960729 Rocky Linux Security Update for container-tools:rhel8 (RLSA-2020:0348)
- 960813 Rocky Linux Security Update for container-tools:1.0 (RLSA-2020:1360)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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**