



CVE-2020-8608

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

Summary

CVE	CVE-2020-8608
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-06 17:15:00 UTC
Updated	2021-02-14 03:50:00 UTC
Description	In libslirp 4.1.0, as used in QEMU 4.2.0, tcp_subr.c misuses sprintf return values, leading to a buffer overflow in later code

Risk And Classification

Problem Types: CWE-120

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	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	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

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-4733-1 qemu	DEBIAN	www.debian.org	This
USN-4283-1: QEMU vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	This
CVE-2020-8608 QEMU Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	This
v4.1.0 · Tags · slirp / libslirp · GitLab	MISC	gitlab.freedesktop.org	Re

[SECURITY] [DLA 2551-1] slirp security update	MLIST	lists.debian.org	Ma
tcp_emu: fix unsafe snprintf() usages (68ccb802) · Commits · slirp / libslirp · GitLab	MISC	gitlab.freedesktop.org	Pa
[SECURITY] [DLA 2288-1] qemu security update	MLIST	lists.debian.org	Ma
[SECURITY] [DLA 2142-1] slirp security update	MLIST	lists.debian.org	Thi
[SECURITY] [DLA 2144-1] qemu security update	MLIST	lists.debian.org	Thi
oss-security - CVE-2020-8608 QEMU: Slirp: potential OOB access due to unsafe snprintf() usages	MISC	www.openwall.com	Ma
QEMU: Multiple vulnerabilities (GLSA 202003-66) — Gentoo security	GENTOO	security.gentoo.org	Thi
[security-announce] openSUSE-SU-2020:0468-1: important: Security update	SUSE	lists.opensuse.org	Ma
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [377058](#) Alibaba Cloud Linux Security Update for qemu-kvm-ma (ALINUX2-SA-2020:0067)
- [377221](#) Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2020:0074)
- [377335](#) Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2022:0110)
- [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)
- [750124](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1894-1)
- [750129](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1895-1)
- [750138](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1918-1)
- [750149](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1942-1)
- [750152](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1947-1)
- [750771](#) OpenSUSE Security Update for qemu (openSUSE-SU-2021:1942-1)
- [750827](#) OpenSUSE Security Update for qemu (openSUSE-SU-2021:1043-1)
- [940423](#) AlmaLinux Security Update for virt:rhel (ALSA-2020:2774)
- [940515](#) AlmaLinux Security Update for container-tools:rhel8 (ALSA-2020:1379)
- [960750](#) Rocky Linux Security Update for virt:rhel (RLSA-2020:2774)
- [960875](#) Rocky Linux Security Update for container-tools:rhel8 (RLSA-2020:1379)

© [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](#)