CVE-2019-6778

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-6778
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:01:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	In QEMU 3.0.0, tcp_emu in slirp/tcp_subr.c has a heap-based buffer overflow.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	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	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	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	18.10	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Application	Qemu	Qemu	3.0.0	All	All	All

Application	Qemu	Qemu	3.0.0	All	All	All

References

Reference	Source	Link	Tag
[security-announce] openSUSE-SU-2019:0254-1: important: Security update	SUSE	lists.opensuse.org	Mail
oss-security - CVE-2019-6778 QEMU: slirp: heap buffer overflow in tcp_emu()	MISC	www.openwall.com	Mail
[SECURITY] Fedora 29 Update: qemu-3.0.0-4.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Mail
[security-announce] openSUSE-SU-2019:1226-1: important: Security update	SUSE	lists.opensuse.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
[security-announce] openSUSE-SU-2019:1074-1: important: Security update	SUSE	lists.opensuse.org	Mail
[security-announce] openSUSE-SU-2019:2044-1: moderate: Security update f	SUSE	lists.opensuse.org	
[SECURITY] Fedora 30 Update: qemu-3.1.0-6.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Mail
[SECURITY] Fedora 30 Update: qemu-3.1.0-6.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
[SECURITY] Fedora 29 Update: qemu-3.0.0-4.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
QEMU 'tcp_subr.c' Local Heap Buffer Overflow Vulnerability	BID	www.securityfocus.com	Thir
Debian -- Security Information -- DSA-4454-1 qemu	DEBIAN	www.debian.org	
[Qemu-devel] [PULL 65/65] slirp: check data length while emulating ident	MISC	lists.gnu.org	Mail
USN-3923-1: QEMU vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Thir
Bugtraq: [SECURITY] [DSA 4454-1] qemu security update	BUGTRAQ	seclists.org	
[security-announce] openSUSE-SU-2020:0468-1: important: Security update	SUSE	lists.opensuse.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

377176 Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2019:0045)

377413 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)

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