CVE-2019-14378

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-14378
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-29 11:15:00 UTC
Updated	2023-11-07 03:04:00 UTC
Description	ip_reass in ip_input.c in libslirp 4.0.0 has a heap-based buffer overflow via a large packet because it mishandles a case inv

Risk And Classification

Problem Types: CWE-787 | CWE-755

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libslirp Project	Libslirp	4.0.0	All	All	All
Application	Libslirp Project	Libslirp	4.0.0	All	All	All

References

Reference	Source	Link
QEMU developer here. Some context on the impact and the security architecture o... | Hacker News	MISC	news.ycombinator.com
[SECURITY] [DLA 1927-1] qemu security update	MLIST	lists.debian.org
QEMU VM Escape | bi0s	MISC	blog.bi0s.in
Bugtraq: [SECURITY] [DSA 4512-1] qemu security update	BUGTRAQ	seclists.org
[security-announce] openSUSE-SU-2019:2510-1: important: Security update	SUSE	lists.opensuse.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Debian -- Security Information -- DSA-4506-1 qemu	DEBIAN	www.debian.org
[security-announce] openSUSE-SU-2019:2041-1: important: Security update	SUSE	lists.opensuse.org
Red Hat Customer Portal	REDHAT	access.redhat.com

[SECURITY] Fedora 30 Update: libslirp-4.0.0-2.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Bugtraq: [SECURITY] [DSA 4506-1] qemu security update	BUGTRAQ	seclists.org
Red Hat Customer Portal - Access to 24x7 support and knowledge	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Fix heap overflow in ip_reass on big packet input (126c04ac) · Commits · slirp / libslirp · GitLab	MISC	gitlab.freedesktop.org
[security-announce] openSUSE-SU-2019:2059-1: important: Security update	SUSE	lists.opensuse.org
support.f5.com/csp/article/K25423748	CONFIRM	support.f5.com
support.f5.com/csp/article/K25423748	CONFIRM	support.f5.com
USN-4191-1: QEMU vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	REDHAT	access.redhat.com
myF5		support.f5.com
Red Hat Customer Portal	REDHAT	access.redhat.com
oss-security - CVE-2019-14378 QEMU: slirp: heap buffer overflow during packet reassembly	MLIST	www.openwall.com
QEMU Denial Of Service ≈ Packet Storm	MISC	packetstormsecurity.com
Debian -- Security Information -- DSA-4512-1 qemu	DEBIAN	www.debian.org
USN-4191-2: QEMU vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com
[SECURITY] Fedora 30 Update: libslirp-4.0.0-2.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.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

- 159649 Oracle Enterprise Linux Security Update for container-tools:1.0 security and bug fix update (ELSA-2019-3494)
- 159674 Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2019-3403)
- 377172 Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2020:0018)
- 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)
- 940564 AlmaLinux Security Update for container-tools:1.0 (ALSA-2019:3494)
- 940568 AlmaLinux Security Update for container-tools:rhel8 (ALSA-2019:3403)
- 960745 Rocky Linux Security Update for container-tools:rhel8 (RLSA-2019:3403)
- 960831 Rocky Linux Security Update for container-tools:1.0 (RLSA-2019:3494)