



CVE-2020-1983

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-1983
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-22 20:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	A use after free vulnerability in ip_reass() in ip_input.c of libslirp 4.2.0 and prior releases allows crafted packets to cause a c

Risk And Classification

Problem Types: CWE-416

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	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	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	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Libslirp Project	Libslirp	All	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
[SECURITY] Fedora 31 Update: libslirp-4.1.0-2.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	

[security-announce] openSUSE-SU-2020:0636-1: important: Security update	SUSE	lists.opensuse.org	Third
[security-announce] openSUSE-SU-2020:0756-1: moderate: Security update f	SUSE	lists.opensuse.org	
[SECURITY] [DLA 2262-1] qemu security update	MLIST	lists.debian.org	
Merge branch 'cve-2020-1983' into 'master' (9ac0371b) · Commits · slirp / libslirp · GitLab	MISC	gitlab.freedesktop.org	Patch
[SECURITY] Fedora 32 Update: libslirp-4.2.0-2.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third
[SECURITY] [DLA 2288-1] qemu security update	MLIST	lists.debian.org	
USN-4372-1: QEMU vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
Security Disclosure (#20) · Issues · slirp / libslirp · GitLab	MISC	gitlab.freedesktop.org	Explo
[SECURITY] Fedora 32 Update: libslirp-4.2.0-2.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 31 Update: libslirp-4.1.0-2.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third
Debian -- Security Information -- DSA-4665-1 qemu	DEBIAN	www.debian.org	Third
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered by Aviv Sasson of Palo Alto Networks.

Legacy QID Mappings

- [159669](#) Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2020-4676)
- [239166](#) Red Hat Update for qemu-kvm-rhev (RHSA-2021:0934)
- [377063](#) Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2020:0120)
- [377247](#) Alibaba Cloud Linux Security Update for qemu-kvm-ma (ALINUX2-SA-2021:0007)
- [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)
- [501608](#) Alpine Linux Security Update for libslirp
- [940165](#) AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2020:4676)
- [940565](#) AlmaLinux Security Update for container-tools:rhel8 (ALSA-2020:3053)
- [960273](#) Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2020:4676)
- [960335](#) Rocky Linux Security Update for container-tools:rhel8 (RLSA-2020:3053)

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](#)