



CVE-2019-15890

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

Summary

CVE	CVE-2019-15890
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-06 17:15:00 UTC
Updated	2019-09-20 11:15:00 UTC
Description	libslirp 4.0.0, as used in QEMU 4.1.0, has a use-after-free in ip_reass in ip_input.c.

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libslirp Project	Libslirp	4.0.0	-	All	All
Application	Libslirp Project	Libslirp	4.0.0	-	All	All
Application	Qemu	Qemu	4.1.0	All	All	All
Application	Qemu	Qemu	4.1.0	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 1927-1] qemu security update	MLIST	lists.debian.org	
[security-announce] openSUSE-SU-2019:2510-1: important: Security update	SUSE	lists.opensuse.org	
Bugtraq: [SECURITY] [DSA 4616-1] qemu security update	BUGTRAQ	seclists.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
oss-security - CVE-2019-15890 QEMU: Slirp: use-after-free during packet reassembly	CONFIRM	www.openwall.com	Mailing List, Pa
Debian -- Security Information -- DSA-4616-1 qemu	DEBIAN	www.debian.org	
USN-4191-1: QEMU vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
ip_reass: Fix use after free (c5927943) · Commits · slirp / libslirp · GitLab	MISC	gitlab.freedesktop.org	Patch, Third Pa
USN-4191-2: QEMU vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159669 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2020-4676)
296075 Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)
377413 Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)
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)
940165 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2020:4676)
940555 AlmaLinux Security Update for container-tools:rhel8 (ALSA-2020:0348)
960273 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2020:4676)
960729 Rocky Linux Security Update for container-tools:rhel8 (RLSA-2020:0348)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report