



# CVE-2020-29130

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-29130
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-26 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:21:00 UTC
<b>Description</b>	slirp.c in libslirp through 4.3.1 has a buffer over-read because it tries to read a certain amount of header data even if that ex

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Libslirp Project</a>	<a href="#">Libslirp</a>	All	All	All	All

## References

Reference	Source	Lin
[SECURITY] Fedora 33 Update: libslirp-4.3.1-3.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists</a>
[Slirp] [PATCH] slirp: check pkt_len before reading protocol header	MISC	<a href="#">lists</a>
[SECURITY] [DLA 3362-1] qemu security update	MLIST	<a href="#">lists</a>
[SECURITY] [DLA 2560-1] qemu security update	MLIST	<a href="#">lists</a>
[SECURITY] Fedora 33 Update: libslirp-4.3.1-3.fc33 - package-announce - Fedora Mailing-Lists		<a href="#">lists</a>
[SECURITY] Fedora 32 Update: libslirp-4.3.1-3.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists</a>
[SECURITY] Fedora 32 Update: libslirp-4.3.1-3.fc32 - package-announce - Fedora Mailing-Lists		<a href="#">lists</a>

oss-security - CVE-2020-29129 CVE-2020-29130 QEMU: slirp: out-of-bounds access while processing ARP/NCSI packets	MLIST	<a href="#">ww</a>
CVE Program record	CVE.ORG	<a href="#">ww</a>
NVD vulnerability detail	NVD	<a href="#">nvc</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [159456](#) Oracle Enterprise Linux Security Update for virt:ol and virt-devel:rhel (ELSA-2021-1762)
- [159582](#) Oracle Enterprise Linux Security Update for qemu (ELSA-2021-9638)
- [159672](#) Oracle Enterprise Linux Security Update for kvm\_utils (ELSA-2022-9172)
- [174920](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1243-1)
- [174921](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1245-1)
- [174922](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1240-1)
- [174923](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1241-1)
- [174924](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1244-1)
- [174926](#) SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2021:1242-1)
- [181630](#) Debian Security Update for qemu (DLA 3362-1)
- [198431](#) Ubuntu Security Notification for libslirp vulnerabilities (USN-5009-1)
- [239306](#) Red Hat Update for virt:rhel and virt-devel:rhel (RHSA-2021:1762)
- [352383](#) Amazon Linux Security Advisory for qemu: ALAS2-2021-1671
- [377413](#) Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)
- [501610](#) Alpine Linux Security Update for libslirp
- [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)
- [750251](#) OpenSUSE Security Update for qemu (openSUSE-SU-2021:0600-1)

<a href="#">750771</a> OpenSUSE Security Update for qemu (openSUSE-SU-2021:1942-1)
<a href="#">750827</a> OpenSUSE Security Update for qemu (openSUSE-SU-2021:1043-1)
<a href="#">751924</a> OpenSUSE Security Update for slirp4netns (openSUSE-SU-2022:0943-1)
<a href="#">753108</a> SUSE Enterprise Linux Security Update for slirp4netns (SUSE-SU-2022:0943-1)
<a href="#">940118</a> AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:1762)
<a href="#">960265</a> Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:1762)

© [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](#)**