CVE-2020-29129

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-29129
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-26 20:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	ncsi.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	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Libslirp Project	Libslirp	All	All	All	All

References

Reference	Source	Lin
[SECURITY] Fedora 33 Update: libslirp-4.3.1-3.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists
[Slirp] [PATCH] slirp: check pkt_len before reading protocol header	MISC	lists
[SECURITY] [DLA 3099-1] qemu security update	MLIST	lists
[SECURITY] Fedora 33 Update: libslirp-4.3.1-3.fc33 - package-announce - Fedora Mailing-Lists		lists
[SECURITY] Fedora 32 Update: libslirp-4.3.1-3.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists
[SECURITY] Fedora 32 Update: libslirp-4.3.1-3.fc32 - package-announce - Fedora Mailing-Lists		lists
oss-security - CVE-2020-29129 CVE-2020-29130 QEMU: slirp: out-of-bounds access while processing ARP/NCSI packets	MLIST	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

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)

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)

180995 Debian Security Update for qemu (DLA 3099-1)

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

501610 Alpine Linux Security Update for libslirp

671198 EulerOS Security Update for qemu (EulerOS-SA-2022-1034)

671203 EulerOS Security Update for qemu (EulerOS-SA-2022-1014)

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)

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)

750771 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1942-1)

750827 OpenSUSE Security Update for qemu (openSUSE-SU-2021:1043-1)

940118 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2021:1762)

960265 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2021:1762)

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