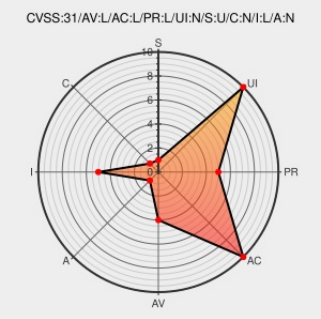
CVE-2019-17054

Published on: 10/01/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:06:00 AM UTC

CVE-2019-17054

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

atalk_create in net/appletalk/ddp.c in the AF_APPLETALK network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-6cc03e8aa36c.

CVE-2019-17054 has been assigned by cve@mitre.org to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.3 - LOW

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	LOW	NONE

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-311-01)	seclists.org text/html	BUGTRAQ 20191108 [slackware-security] Slackware 14.2 kernel (SSA:2019-311-01)
USN-4185-2: Linux kernel (Azure) vulnerabilities | Ubuntu security notices |	usn.ubuntu.com text/html	UBUNTU USN-4185-2

Ubuntu		
[SECURITY] [DLA 2114-1] linux-4.9 security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200302 [SECURITY] [DLA 2114-1] linux-4.9 security update
USN-4185-1: Linux kernel vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-4185-1
Slackware Security Advisory - Slackware 14.2 kernel Updates ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155212/Slackware-Security-Advisory-Slackware-14.2-kernel-Updates.html
[SECURITY] Fedora 29 Update: kernel-headers-5.3.6-100.fc29 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-41e28660ae
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=0edc3f703f7bcaf550774b5d43ab727bcd0fe06b
USN-4186-1: Linux kernel vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-4186-1
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6cc03e8aa36c51f3b26a0d21a3c4ce2809c842ac
USN-4186-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4186-2
USN-4184-1: Linux kernel vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-4184-1
[SECURITY] [DLA 2068-1] linux security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200118 [SECURITY] [DLA 2068-1] linux security update

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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