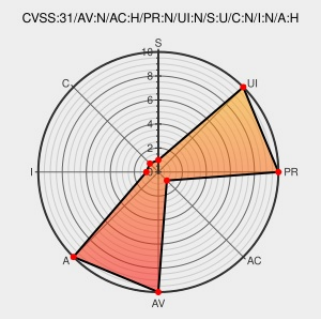
CVE-2019-19076

Published on: 11/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19076

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

** DISPUTED ** A memory leak in the nfp_abm_u32_knode_replace() function in drivers/net/ethernet/netronome/nfp/abm/cls.c in the Linux kernel before 5.3.6 allows attackers to cause a denial of service (memory consumption), aka CID-78beef629fd9. NOTE: This has been argued as not a valid vulnerability. The upstream commit 78beef629fd9 was reverted.

CVE-2019-19076 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 7.1 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Re: [PATCH v3] nfp: abm: fix memory leak in	Patch Vendor Advisory	MISC lore.kernel.org/lkml/20191204103955.63c4d9af@cakuba.netronome.com/

nfp_abm_u32_knode_replace - Jakub Kicinski	lore.kernel.org text/html	
USN-4209-1: Linux kernel vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-4209-1
November 2019 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	Third Party Advisory security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20191205-0001/
nfp: abm: fix memory leak in nfp_abm_u32_knode_replace · torvalds/linux@78beef6 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/78beef629fd95be4ed853b2d37b832f766bd96ca
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/linus/1d1997db870f4058676439ef7014390ba9e24eb2
	Release Notes Vendor Advisory cdn.kernel.org text/plain	MISC cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.6

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→