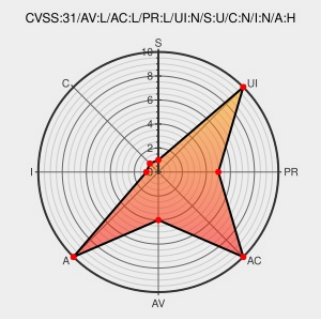
CVE-2019-20422

Published on: 01/26/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:50 PM UTC

CVE-2019-20422

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



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

In the Linux kernel before 5.3.4, fib6_rule_lookup in net/ipv6/ip6_fib.c mishandles the RT6_LOOKUP_F_DST_NOREF flag in a reference-count decision, leading to (for example) a crash that was identified by syzkaller, aka CID-7b09c2d052db.

CVE-2019-20422 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
	Mailing List Vendor Advisory cdn.kernel.org text/plain	MISC cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.4

ipv6: fix a typo in fib6_rule_lookup() · torvalds/linux@7b09c2d · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/7b09c2d052db4b4ad0b27b97918b46a7746966fa
February 2020 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20200313-0003/

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
Operating System	Linux	Linux Kernel	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→