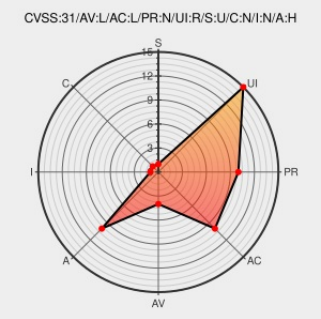
CVE-2019-19815

Published on: 12/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:53 PM UTC

CVE-2019-19815

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



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

In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause a NULL pointer dereference in f2fs_recover_fsync_data in fs/f2fs/recovery.c. This is related to F2FS_P_SB in fs/f2fs/f2fs.h.

CVE-2019-19815 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	NONE	REQUIRED
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
f2fs: support swap file w/ DIO · torvalds/linux@4969c06 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/4969c06a0d83c9c3dc50b8efcdc8eeedfce896f6#diff-41a7fa4590d2af87e82101f2b4dadb56

December 2019 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20200103-0001/
CVE/CVE-2019-19815 at master · bobfuzzer/CVE · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/bobfuzzer/CVE/tree/master/CVE-2019-19815

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	5.0.21	All	All	All
Operating System	Linux	Linux Kernel	5.0.21	All	All	All

cpe:2.3:o:linux:linux_kernel:5.0.21:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:5.0.21:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→