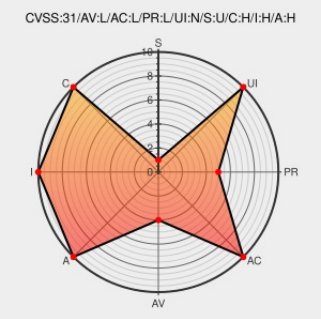
CVE-2019-18675

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 02/24/2023 06:42:00 PM UTC

CVE-2019-18675

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



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

The Linux kernel through 5.3.13 has a start_offset+size Integer Overflow in cpia2_remap_buffer in drivers/media/usb/cpia2/cpia2_core.c because cpia2 has its own mmap implementation. This allows local users (with /dev/video0 access) to obtain read and write permissions on kernel physical pages, which can possibly result in a privilege escalation.

CVE-2019-18675 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
December 2019 Linux Kernel Vulnerabilities in	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20200103-0001/

NetApp Products | NetApp Product Security		
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/log/drivers/media/usb/cpia2/cpia2_c
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	CONFIRM git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=be83bbf806822b1b89e0a0f23cd87cddc409e429
mmap handler exploitation	Exploit Third Party Advisory deshal3v.github.io text/html	MISC deshal3v.github.io/blog/kernel-research/mmap_exploitation

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→