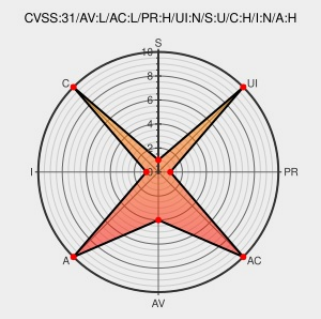
CVE-2019-19927

Published on: 12/30/2019 12:00:00 AM UTC

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

CVE-2019-19927

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



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

In the Linux kernel 5.0.0-rc7 (as distributed in ubuntu/linux.git on kernel.ubuntu.com), mounting a crafted f2fs filesystem image and performing some operations can lead to slab-out-of-bounds read access in ttm_put_pages in drivers/gpu/drm/ttm/ttm_page_alloc.c. This is related to the vmwgfx or ttm module.

CVE-2019-19927 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6 - MEDIUM

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

CVSS2 Score: 3.6 - LOW

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

CVE References

Description	Tags	Link
drm/ttm: fix incrementing the page pointer for huge pages · torvalds/linux@4533933 · GitHub	Patch, Third Party Advisory, github.com	MISC github.com/torvalds/linux/commit/453393369dc9806d2455151e329c599684762428

GitHub	text/html	
drm/ttm: fix start page for huge page check in ttm_put_pages() · torvalds/linux@ac1e516 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/ac1e516d5a4c56bf0cb4a3dfc0672f689131cfd4
January 2020 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	Third Party Advisory security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20200204-0002/
CVE/CVE-2019-19927 at master · bobfuzzer/CVE · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/bobfuzzer/CVE/tree/master/CVE-2019-19927
drm/ttm: fix out-of-bounds read in ttm_put_pages() v2 · torvalds/linux@a66477b · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/a66477b0efe511d98dde3e4aaeb189790e6f0a39
[security-announce] openSUSE-SU-2020:0336-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0336

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	rc7	All	All
Operating System	Linux	Linux Kernel	5.0	rc7	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

cpe:2.3:o:linux:linux_kernel:5.0:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:5.0:rc7:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→