

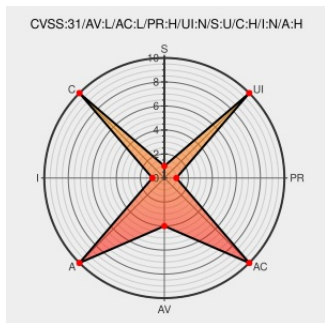


CVE-2019-19927

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 [M](#) 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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)