Bug 1876995 (CVE-2020-25639) - CVE-2020-25639 kernel: NULL pointer dereference via nouveau ioctl can lead to DoS

Keywords:	Security ×
Status:	CLOSED WONTFIX
Alias:	CVE-2020-25639
Product:	Security Response
Component:	vulnerability
Version:	unspecified
Hardware:	All
OS:	Linux
Priority:	low
Severity:	low
Target Milestone:	---
Assignee:	Red Hat Product Security
QA Contact:	
Docs Contact:	
URL:	
Whiteboard:	
Depends On:	1935209 1877471 1877472 ~~1881465~~ 1911194
Blocks:	1873622
TreeView+	depends on / blocked

Reported:	2020-09-08 16:51 UTC by Guilherme de Almeida Suckevicz
Modified:	2021-11-07 11:30 UTC (History)
CC List:	47 users (show)
Fixed In Version:	Linux kernel 5.12-rc1
Doc Type:	If docs needed, set a value
Doc Text:	A NULL pointer dereference flaw was found in the Linux kernel’s GPU Nouveau driver functionality in the way the user calls ioctl DRM_IOCTL_NOUVEAU_CHANNEL_ALLOC. This flaw allows a local user to crash the system.
Clone Of:	
Environment:	
Last Closed:	2021-11-07 11:23:48 UTC

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Guilherme de Almeida Suckevicz 2020-09-08 16:51:13 UTC — Description

A flaw was found in the Linux kernel where an unprivileged console user can crash kernel via a nouveau ioctl.

Reference:
https://lists.freedesktop.org/archives/nouveau/2020-August/036682.html

Alex 2020-09-21 20:07:32 UTC — Comment 4

Acknowledgments:

Name: Frantisek Hrbata (Red Hat)

Alex 2020-09-22 13:10:08 UTC — Comment 6

Created kernel tracking bugs for this issue:

Affects: fedora-all [~~bug 1881465~~]

RaTasha Tillery-Smith 2020-09-29 19:41:49 UTC — Comment 7

Statement:

This flaw is rated as having a Low impact because the issue can only be triggered by an authorized local user in the render group.

Alex 2020-12-09 16:34:48 UTC — Comment 10

Mitigation:

To mitigate this issue, prevent the module nouveau from being loaded. Please see https://access.redhat.com/solutions/41278 for information on how to blacklist a kernel module to prevent it from loading automatically.

Karol Herbst 2021-10-26 15:10:40 UTC — Comment 25

Fixed upstream with eaba3b28401f5

Alex 2021-11-07 11:23:48 UTC — Comment 26

Before closing, checked that for the rhel-9 already applied.

Note
You need to log in before you can comment on or make changes to this bug.