



[oss-sec](#) mailing list archives



◀ [By Date](#) ▶    ◀ [By Thread](#) ▶



## Linux kernel: A concurrency use-after-free in floppy's raw\_cmd

*From:* Minh Yuan <yuanmingbuaa () gmail com>

*Date:* Thu, 28 Apr 2022 11:19:46 +0800

Hi,

We recently discovered a concurrency uaf between `raw_cmd_ioctl` and `seek_interrupt` in the latest kernel version (5.17.4 for now).

The root cause is that after deallocating `raw_cmd` in `raw_cmd_ioctl`, `seek_interrupt` still holds the freed `raw_cmd` and accesses it in `floppy_ready` or `start_motor` concurrently.

PoC (generated by syzkaller) is in the attachment, and here is the KASAN report:

BUG: KASAN: use-after-free in `start_motor+0x31b/0x3f0`  
`drivers/block/floppy.c:1908`

Read of size 4 at addr ffff888127331c00 by task kworker/u16:9/15911

CPU: 5 PID: 15911 Comm: kworker/u16:9 Not tainted 5.16.2 #20

Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS

rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014

Workqueue: floppy floppy\_work\_workfn

Call Trace:

<TASK>

\_\_dump\_stack lib/dump\_stack.c:88 [inline]

dump\_stack\_lvl+0xcd/0x134 lib/dump\_stack.c:106

print\_address\_description.constprop.0.cold+0x8d/0x320 mm/kasan/report.c:247

\_\_kasan\_report mm/kasan/report.c:433 [inline]

kasan\_report.cold+0x83/0xdf mm/kasan/report.c:450

start\_motor+0x31b/0x3f0 drivers/block/floppy.c:1908

floppy\_ready+0x83/0x1850 drivers/block/floppy.c:1935

seek\_interrupt+0x326/0x420 drivers/block/floppy.c:1567

process\_one\_work+0x9b2/0x1660 kernel/workqueue.c:2317

worker\_thread+0x65d/0x1130 kernel/workqueue.c:2465

kthread+0x405/0x4f0 kernel/kthread.c:327

ret\_from\_fork+0x1f/0x30 arch/x86/entry/entry\_64.S:295

</TASK>

Allocated by task 22033:

kasan\_save\_stack+0x1e/0x50 mm/kasan/common.c:38

kasan\_set\_track mm/kasan/common.c:46 [inline]

set\_alloc\_info mm/kasan/common.c:434 [inline]

```
____kasan_kmalloc mm/kasan/common.c:513 [inline]
____kasan_kmalloc mm/kasan/common.c:472 [inline]
____kasan_kmalloc+0xa9/0xd0 mm/kasan/common.c:522
kmalloc include/linux/slab.h:590 [inline]
raw_cmd_copyin drivers/block/floppy.c:3100 [inline]
raw_cmd_ioctl drivers/block/floppy.c:3167 [inline]
fd_locked_ioctl+0x100e/0x2820 drivers/block/floppy.c:3535
fd_ioctl+0x35/0x50 drivers/block/floppy.c:3562
blkdev_ioctl+0x37a/0x800 block/ioctl.c:609
vfs_ioctl fs/ioctl.c:51 [inline]
__do_sys_ioctl fs/ioctl.c:874 [inline]
__se_sys_ioctl fs/ioctl.c:860 [inline]
__x64_sys_ioctl+0x193/0x200 fs/ioctl.c:860
do_syscall_x64 arch/x86/entry/common.c:50 [inline]
do_syscall_64+0x35/0x80 arch/x86/entry/common.c:80
entry_SYSCALL_64_after_hwframe+0x44/0xae
```

Freed by task 22033:

```
kasan_save_stack+0x1e/0x50 mm/kasan/common.c:38
kasan_set_track+0x21/0x30 mm/kasan/common.c:46
kasan_set_free_info+0x20/0x30 mm/kasan/generic.c:370
____kasan_slab_free mm/kasan/common.c:366 [inline]
____kasan_slab_free mm/kasan/common.c:328 [inline]
__kasan_slab_free+0xff/0x130 mm/kasan/common.c:374
kasan_slab_free include/linux/kasan.h:235 [inline]
slab_free_hook mm/slub.c:1723 [inline]
slab_free_freelist_hook+0x8b/0x1c0 mm/slub.c:1749
slab_free mm/slub.c:3513 [inline]
kfree+0xf6/0x560 mm/slub.c:4561
raw_cmd_free+0x8a/0x1c0 drivers/block/floppy.c:3086
raw_cmd_ioctl drivers/block/floppy.c:3187 [inline]
fd_locked_ioctl+0x206d/0x2820 drivers/block/floppy.c:3535
fd_ioctl+0x35/0x50 drivers/block/floppy.c:3562
blkdev_ioctl+0x37a/0x800 block/ioctl.c:609
vfs_ioctl fs/ioctl.c:51 [inline]
__do_sys_ioctl fs/ioctl.c:874 [inline]
__se_sys_ioctl fs/ioctl.c:860 [inline]
__x64_sys_ioctl+0x193/0x200 fs/ioctl.c:860
do_syscall_x64 arch/x86/entry/common.c:50 [inline]
do_syscall_64+0x35/0x80 arch/x86/entry/common.c:80
entry_SYSCALL_64_after_hwframe+0x44/0xae
```

The new patch can be seen at

<https://github.com/torvalds/linux/commit/233087ca063686964a53c829d547c7571e3f67bf>

.

Regards,

Yuan Ming from Tsinghua University

**Attachment:** [floppy\\_poc.c](#)

*Description:*

---

 [By Date](#)   [By Thread](#) 

**Current thread:**

**Linux kernel: A concurrency use-after-free in floppy's raw\_cmd** *Minh Yuan (Apr 28)*



## Nmap Security Scanner

[Ref Guide](#)[Install Guide](#)[Docs](#)[Download](#)[Nmap OEM](#)

## Npcap packet capture

[User's Guide](#)[API docs](#)[Download](#)[Npcap OEM](#)

## Security Lists

[Nmap Announce](#)[Nmap Dev](#)[Full Disclosure](#)[Open Source Security](#)[BreachExchange](#)

## Security Tools

[Vuln scanners](#)[Password audit](#)[Web scanners](#)[Wireless](#)[Exploitation](#)

## About

[About/Contact](#)[Privacy](#)[Advertising](#)[Nmap Public Source License](#)