From Kyungtae Kim <>
Date Mon, 23 Mar 2020 02:16:43 -0400
Subject BUG: KASAN: use-after-free in usb_hcd_unlink_urb+0x5f/0x170 drivers/usb/core/hcd.c

```
We report a bug (in linux-5.5.11) found by FuzzUSB (a modified version
of syzkaller)

In function usb_hcd_unlink_urb (driver/usb/core/hcd.c:1607), it tries to
read "urb->use_count". But it seems the instance "urb" was
already freed (right after urb->dev at line 1597) by the function "urb_destroy"
in a different thread, which caused memory access violation.
To solve, it may need to check if urb is valid before urb->use_count,
to avoid such freed memory access.

kernel config: https://kt0755.github.io/etc/config_v5.5.11

==================================================================
BUG: KASAN: use-after-free in atomic_read
include/asm-generic/atomic-instrumented.h:26 [inline]
BUG: KASAN: use-after-free in usb_hcd_unlink_urb+0x5f/0x170
drivers/usb/core/hcd.c:1607
Read of size 4 at addr ffff888065379610 by task kworker/u4:1/27

CPU: 1 PID: 27 Comm: kworker/u4:1 Not tainted 5.5.11 #2
Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS
1.10.2-1ubuntu1 04/01/2014
Workqueue: scsi_tmf_2 scmd_eh_abort_handler
Call Trace:
 __dump_stack lib/dump_stack.c:77 [inline]
 dump_stack+0xce/0x128 lib/dump_stack.c:118
 print_address_description.constprop.4+0x21/0x3c0 mm/kasan/report.c:374
 __kasan_report+0x153/0x1cb mm/kasan/report.c:506
 kasan_report+0x12/0x20 mm/kasan/common.c:639
 check_memory_region_inline mm/kasan/generic.c:185 [inline]
 check_memory_region+0x152/0x1b0 mm/kasan/generic.c:192
 __kasan_check_read+0x11/0x20 mm/kasan/common.c:95
 atomic_read include/asm-generic/atomic-instrumented.h:26 [inline]
 usb_hcd_unlink_urb+0x5f/0x170 drivers/usb/core/hcd.c:1607
 usb_unlink_urb+0x72/0xb0 drivers/usb/core/urb.c:657
 usb_sg_cancel+0x14e/0x290 drivers/usb/core/message.c:602
 usb_stor_stop_transport+0x5e/0xa0 drivers/usb/storage/transport.c:937
 command_abort+0x19d/0x200 drivers/usb/storage/scsiglue.c:439
 scsi_try_to_abort_cmd drivers/scsi/scsi_error.c:927 [inline]
 scmd_eh_abort_handler+0x18e/0x410 drivers/scsi/scsi_error.c:145
 process_one_work+0x9dd/0x1710 kernel/workqueue.c:2266
 worker_thread+0x8b/0xc40 kernel/workqueue.c:2412
 kthread+0x35f/0x440 kernel/kthread.c:255
 ret_from_fork+0x24/0x30 arch/x86/entry/entry_64.S:352

Allocated by task 2532:
 save_stack+0x21/0x90 mm/kasan/common.c:72
 set_track mm/kasan/common.c:80 [inline]
 __kasan_kmalloc.constprop.3+0xa7/0xd0 mm/kasan/common.c:513
 kasan_kmalloc+0x9/0x10 mm/kasan/common.c:527
 __kmalloc+0x148/0x380 mm/slub.c:3812
 kmalloc include/linux/slab.h:561 [inline]
 usb_alloc_urb+0x42/0x90 drivers/usb/core/urb.c:74
 usb_sg_init+0x323/0xa00 drivers/usb/core/message.c:406
 usb_stor_bulk_transfer_sglist+0xbe/0x280 drivers/usb/storage/transport.c:423
 usb_stor_bulk_srb+0x10d/0x230 drivers/usb/storage/transport.c:465
 usb_stor_Bulk_transport+0x55f/0x1060 drivers/usb/storage/transport.c:1161
 usb_stor_invoke_transport+0xef/0x15f0 drivers/usb/storage/transport.c:606
 usb_stor_transparent_scsi_command+0x1d/0x30 drivers/usb/storage/protocol.c:108
 usb_stor_control_thread+0x6d8/0xa80 drivers/usb/storage/usb.c:380
 kthread+0x35f/0x440 kernel/kthread.c:255
 ret_from_fork+0x24/0x30 arch/x86/entry/entry_64.S:352

Freed by task 2532:
 save_stack+0x21/0x90 mm/kasan/common.c:72
 set_track mm/kasan/common.c:80 [inline]
 kasan_set_free_info mm/kasan/common.c:335 [inline]
 __kasan_slab_free+0x135/0x190 mm/kasan/common.c:474
 kasan_slab_free+0xe/0x10 mm/kasan/common.c:483
 slab_free_hook mm/slub.c:1425 [inline]
 slab_free_freelist_hook mm/slub.c:1458 [inline]
 slab_free mm/slub.c:3005 [inline]
 kfree+0xf7/0x410 mm/slub.c:3966
 urb_destroy drivers/usb/core/urb.c:26 [inline]
 kref_put include/linux/kref.h:65 [inline]
 usb_free_urb.part.0+0x95/0x100 drivers/usb/core/urb.c:96
 usb_free_urb+0x1f/0x30 drivers/usb/core/urb.c:95
 sg_clean+0x111/0x270 drivers/usb/core/message.c:263
 usb_sg_wait+0x26d/0x440 drivers/usb/core/message.c:573
 usb_stor_bulk_transfer_sglist+0x127/0x280 drivers/usb/storage/transport.c:447
 usb_stor_bulk_srb+0x10d/0x230 drivers/usb/storage/transport.c:465
 usb_stor_Bulk_transport+0x55f/0x1060 drivers/usb/storage/transport.c:1161
 usb_stor_invoke_transport+0xef/0x15f0 drivers/usb/storage/transport.c:606
 usb_stor_transparent_scsi_command+0x1d/0x30 drivers/usb/storage/protocol.c:108
 usb_stor_control_thread+0x6d8/0xa80 drivers/usb/storage/usb.c:380
 kthread+0x35f/0x440 kernel/kthread.c:255
 ret_from_fork+0x24/0x30 arch/x86/entry/entry_64.S:352

The buggy address belongs to the object at ffff888065379600
 which belongs to the cache kmalloc-192 of size 192
The buggy address is located 16 bytes inside of
 192-byte region [ffff888065379600, ffff8880653796c0)
The buggy address belongs to the page:
page:ffffea000194de40 refcount:1 mapcount:0 mapping:ffff88806c002a00 index:0x0
flags: 0x100000000000200(slab)
raw: 0100000000000200 ffffea0000ee7a00 0000000500000005 ffff88806c002a00
raw: 0000000000000000 0000000080100010 00000001ffffffff 0000000000000000
page dumped because: kasan: bad access detected

Memory state around the buggy address:
 ffff888065379500: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
 ffff888065379580: fb fb fb fb fb fb fb fb fc fc fc fc fc fc fc fc
>ffff888065379600: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb
                   ^
 ffff888065379680: fb fb fb fb fb fb fb fb fc fc fc fc fc fc fc fc
 ffff888065379700: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
==================================================================
```