From: Rondreis <linhaoguo86@gmail.com>
To: stern@rowland.harvard.edu, linux-usb@vger.kernel.org,
linux-kernel@vger.kernel.org
Subject: kernel v5.19 warn in usb_composite_setup_continue
Date: Thu, 11 Aug 2022 10:02:26 +0800 [thread overview]
Message-ID: <CAB7eexLLApHJwZfMQ=X-PtRhw0BgO+5KcSMS05FNUYejJXqtSA@mail.gmail.com> (raw)

Hello,

When fuzzing the Linux kernel driver 5.19.0-rc4-00208-g69cb6c6556ad,
the following crash was triggered.

HEAD commit: 4b0986a3613c92f4ec1bdc7f60ec66fea135991f (HEAD, tag: v5.18)
git tree: upstream

kernel config: https://pastebin.com/KecL2gaG
C reproducer: https://pastebin.com/gTWJQwsh
console output: https://pastebin.com/iHzBVP3B

Basically, in the c reproducer, we use the gadget module to emulate
the process of attaching a usb device (vendor id: 0x45e, product id:
0x6d, with function: loopback_null).
To reproduce this crash, we utilize a third-party library to emulate
the attaching process: https://github.com/linux-usb-gadgets/libusbgx.
Just clone this repository, make install it, and compile the c
reproducer with ``` gcc crash.c -lusbgx -o crash ``` will do the
trick.

It seems that an error state in struct usb_device trigger such kernel warning.

The crash report is as follow:

```
input: Media Center Ed. eHome Infrared Remote Transceiver (045e:006d)
as /devices/platform/dummy_hcd.5/usb6/6-1/6-1:1.0/rc/rc0/input4
------------[ cut here ]------------
usb 6-1: BOGUS control dir, pipe 80000380 doesn't match bRequestType 40
WARNING: CPU: 0 PID: 2465 at drivers/usb/core/urb.c:410
usb_submit_urb+0x1326/0x1820 drivers/usb/core/urb.c:410
Modules linked in:
CPU: 0 PID: 2465 Comm: kworker/0:2 Not tainted 5.19.0-rc4-00208-g69cb6c6556ad #1
Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS
1.13.0-1ubuntu1.1 04/01/2014
Workqueue: usb_hub_wq hub_event
RIP: 0010:usb_submit_urb+0x1326/0x1820 drivers/usb/core/urb.c:410
Code: 7c 24 40 e8 ac 23 91 fd 48 8b 7c 24 40 e8 b2 70 1b ff 45 89 e8
44 89 f1 4c 89 e2 48 89 c6 48 c7 c7 a0 30 a9 86 e8 48 07 11 02 <0f> 0b
e9 1c f0 ff ff e8 7e 23 91 fd 0f b6 1d 63 22 83 05 31 ff 41
RSP: 0018:ffffc900032becf0 EFLAGS: 00010282
RAX: 0000000000000000 RBX: ffff8881100f3058 RCX: 0000000000000000
RDX: ffffc90004961000 RSI: ffff888114c6d580 RDI: fffff52000657d90
RBP: ffff888105ad90f0 R08: ffffffff812c3638 R09: 0000000000000000
R10: 0000000000000005 R11: ffffed1023504ef1 R12: ffff888105ad9000
R13: 0000000000000040 R14: 0000000080000380 R15: ffff88810ba96500
FS: 0000000000000000(0000) GS:ffff88811a800000(0000) knlGS:0000000000000000
CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 00007ffe810bda58 CR3: 000000010b720000 CR4: 0000000000350ef0
Call Trace:
<TASK>
usb_start_wait_urb+0x101/0x4c0 drivers/usb/core/message.c:58
usb_internal_control_msg drivers/usb/core/message.c:102 [inline]
```

```
usb_control_msg+0x31c/0x4a0 drivers/usb/core/message.c:153
mceusb_gen1_init drivers/media/rc/mceusb.c:1431 [inline]
mceusb_dev_probe+0x258e/0x33f0 drivers/media/rc/mceusb.c:1807
usb_probe_interface+0x310/0x800 drivers/usb/core/driver.c:396
call_driver_probe drivers/base/dd.c:555 [inline]
really_probe drivers/base/dd.c:634 [inline]
really_probe+0x23e/0xa80 drivers/base/dd.c:579
__driver_probe_device+0x338/0x4d0 drivers/base/dd.c:764
driver_probe_device+0x4c/0x1a0 drivers/base/dd.c:794
__device_attach_driver+0x20b/0x2f0 drivers/base/dd.c:917
bus_for_each_drv+0x15f/0x1e0 drivers/base/bus.c:427
__device_attach+0x283/0x490 drivers/base/dd.c:989
bus_probe_device+0x1e4/0x290 drivers/base/bus.c:487
device_add+0xc9b/0x1da0 drivers/base/core.c:3417
usb_set_configuration+0x1019/0x1900 drivers/usb/core/message.c:2170
usb_generic_driver_probe+0x9d/0xe0 drivers/usb/core/generic.c:238
usb_probe_device+0xd9/0x2a0 drivers/usb/core/driver.c:293
call_driver_probe drivers/base/dd.c:555 [inline]
really_probe drivers/base/dd.c:634 [inline]
really_probe+0x23e/0xa80 drivers/base/dd.c:579
__driver_probe_device+0x338/0x4d0 drivers/base/dd.c:764
driver_probe_device+0x4c/0x1a0 drivers/base/dd.c:794
__device_attach_driver+0x20b/0x2f0 drivers/base/dd.c:917
bus_for_each_drv+0x15f/0x1e0 drivers/base/bus.c:427
__device_attach+0x283/0x490 drivers/base/dd.c:989
bus_probe_device+0x1e4/0x290 drivers/base/bus.c:487
device_add+0xc9b/0x1da0 drivers/base/core.c:3417
usb_new_device.cold+0x4b8/0x10ca drivers/usb/core/hub.c:2566
hub_port_connect drivers/usb/core/hub.c:5363 [inline]
hub_port_connect_change drivers/usb/core/hub.c:5507 [inline]
port_event drivers/usb/core/hub.c:5663 [inline]
hub_event+0x232d/0x4180 drivers/usb/core/hub.c:5745
process_one_work+0x9cc/0x1650 kernel/workqueue.c:2289
worker_thread+0x623/0x1070 kernel/workqueue.c:2436
kthread+0x2ef/0x3a0 kernel/kthread.c:376
ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:302
</TASK>


```

Reply instructions:

You may reply publicly to this message via plain-text email
using any one of the following methods:

* Save the following mbox file, import it into your mail client,
  and reply-to-all from there: mbox

  Avoid top-posting and favor interleaved quoting:
  https://en.wikipedia.org/wiki/Posting_style#Interleaved_style

* Reply using the **--to**, **--cc**, and **--in-reply-to**
  switches of git-send-email(1):

  git send-email \
    --in-reply-to='CAB7eexLLApHJwZfMQ=X-PtRhw0BgO+5KcSMS05FNUYejJXqtSA@mail.gmail.com' \

```
    --to=linhaoguo86@gmail.com \
    --cc=linux-kernel@vger.kernel.org \
    --cc=linux-usb@vger.kernel.org \
    --cc=stern@rowland.harvard.edu \
    /path/to/YOUR_REPLY

  https://kernel.org/pub/software/scm/git/docs/git-send-email.html

* If your mail client supports setting the In-Reply-To header
  via mailto: links, try the mailto: link

Be sure your reply has a Subject: header at the top and a blank line before the message body.
```
