



[about](#) [summary](#) [refs](#) [log](#) [tree](#) [commit](#) [diff](#) [stats](#)

author Lorenzo Bianconi <lorenzo@kernel.org> 2023-03-06 18:42:51 +0100
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-03-30 12:50:50 +0200
commit [53edfda851dd1ce41ac049ce2f195dc41dd27cc1](#) (patch)
tree [02c0ff80e6887aac0de6173171f77e435a5c3f70](#)
parent [2d34f27714c97a9786a30b3bb54944d6d8ed612f](#) (diff)
download [linux-53edfda851dd1ce41ac049ce2f195dc41dd27cc1.tar.gz](#)

diff options

context:
space:
mode:

wifi: mt76: connac: do not check WED status for non-mmio devices

[Upstream commit 5683e1488aa9b0805a9403d215e48fed29d6d923]

WED is supported just for mmio devices, so do not check it for usb or sdio devices. This patch fixes the crash reported below:

```
[ 21.946627] wlp0s3u1i3: authenticate with c4:41:1e:f5:2b:1d
[ 22.525298] wlp0s3u1i3: send auth to c4:41:1e:f5:2b:1d (try 1/3)
[ 22.548274] wlp0s3u1i3: authenticate with c4:41:1e:f5:2b:1d
[ 22.557694] wlp0s3u1i3: send auth to c4:41:1e:f5:2b:1d (try 1/3)
[ 22.565885] wlp0s3u1i3: authenticated
[ 22.569502] wlp0s3u1i3: associate with c4:41:1e:f5:2b:1d (try 1/3)
[ 22.578966] wlp0s3u1i3: RX AssocResp from c4:41:1e:f5:2b:1d (capab=0x11 status=30 aid=3)
[ 22.579113] wlp0s3u1i3: c4:41:1e:f5:2b:1d rejected association temporarily; comeback duration 1000 TU (1024 ms)
[ 23.649518] wlp0s3u1i3: associate with c4:41:1e:f5:2b:1d (try 2/3)
[ 23.752528] wlp0s3u1i3: RX AssocResp from c4:41:1e:f5:2b:1d (capab=0x11 status=0 aid=3)
[ 23.797450] wlp0s3u1i3: associated
[ 24.959527] kernel tried to execute NX-protected page - exploit attempt? (uid: 0)
[ 24.959640] BUG: unable to handle page fault for address: ffff88800c223200
[ 24.959706] #PF: supervisor instruction fetch in kernel mode
[ 24.959788] #PF: error_code(0x0011) - permissions violation
[ 24.959846] PGD 2c01067 P4D 2c01067 PUD 2c02067 PMD c2a8063 PTE 800000000c223163
[ 24.959957] Oops: 0011 [#1] PREEMPT SMP
[ 24.960009] CPU: 0 PID: 391 Comm: wpa_supplicant Not tainted 6.2.0-kvm #18
[ 24.960089] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.1-2.fc37 04/01/2014
[ 24.960191] RIP: 0010:0xfffff88800c223200
[ 24.960446] RSP: 0018:ffffc90000ff7698 EFLAGS: 00010282
[ 24.960513] RAX: ffff888028397010 RBX: ffff88800c26e630 RCX: 0000000000000058
[ 24.960598] RDX: ffff88800c26f844 RSI: 0000000000000006 RDI: ffff888028397010
[ 24.960682] RBP: ffff88800ea72f00 R08: 18b873fbab2b964c R09: be06b38235f3c63c
[ 24.960766] R10: 18b873fbab2b964c R11: be06b38235f3c63c R12: 0000000000000001
[ 24.960853] R13: ffff88800c26f84c R14: ffff8880063f0ff8 R15: ffff88800c26e644
[ 24.960950] FS: 00007effcea327c0(0000) GS: ffff88807dc00000(0000) knlGS:0000000000000000
[ 24.961036] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[ 24.961106] CR2: ffff88800c223200 CR3: 000000000eaa2000 CR4: 00000000000006b0
[ 24.961190] Call Trace:
[ 24.961219] <TASK>
[ 24.961245] ? mt76_connac_mcu_add_key+0x2cf/0x310
[ 24.961313] ? mt7921_set_key+0x150/0x200
[ 24.961365] ? drv_set_key+0xa9/0x1b0
[ 24.961418] ? ieee80211_key_enable_hw_accel+0xd9/0x240
[ 24.961485] ? ieee80211_key_replace+0x3f3/0x730
[ 24.961541] ? crypto_shash_setkey+0x89/0xd0
[ 24.961597] ? ieee80211_key_link+0x2d7/0x3a0
[ 24.961664] ? crypto_aead_setauthsize+0x31/0x50
[ 24.961730] ? sta_info_hash_lookup+0xa6/0xf0
[ 24.961785] ? ieee80211_add_key+0x1fc/0x250
[ 24.961842] ? rdev_add_key+0x41/0x140
[ 24.961882] ? nl80211_parse_key+0x6c/0x2f0
[ 24.961940] ? nl80211_new_key+0x24a/0x290
[ 24.961984] ? genl_rcv_msg+0x36c/0x3a0
[ 24.962036] ? rdev_mod_link_station+0xe0/0xe0
[ 24.962102] ? nl80211_set_key+0x410/0x410
[ 24.962143] ? nl80211_pre_doit+0x200/0x200
[ 24.962187] ? genl_bind+0xc0/0xc0
[ 24.962217] ? netlink_rcv_skb+0xaa/0xd0
[ 24.962259] ? genl_rcv+0x24/0x40
```

```
[ 24.962300] ? netlink_unicast+0x224/0x2f0
[ 24.962345] ? netlink_sendmsg+0x30b/0x3d0
[ 24.962388] ? ____sys_sendmsg+0x109/0x1b0
[ 24.962388] ? ____sys_sendmsg+0x109/0x1b0
[ 24.962440] ? __import_iovec+0x2e/0x110
[ 24.962482] ? ____sys_sendmsg+0xbe/0xe0
[ 24.962525] ? mod_objcg_state+0x25c/0x330
[ 24.962576] ? __dentry_kill+0x19e/0x1d0
[ 24.962618] ? call_rcu+0x18f/0x270
[ 24.962660] ? __dentry_kill+0x19e/0x1d0
[ 24.962702] ? __x64_sys_sendmsg+0x70/0x90
[ 24.962744] ? do_syscall_64+0x3d/0x80
[ 24.962796] ? exit_to_user_mode_prepare+0x1b/0x70
[ 24.962852] ? entry_SYSCALL_64_after_hwframe+0x46/0xb0
[ 24.962913] </TASK>
[ 24.962939] Modules linked in:
[ 24.962981] CR2: ffff88800c223200
[ 24.963022] ---[ end trace 0000000000000000 ]---
[ 24.963087] RIP: 0010:0xfffff88800c223200
[ 24.963323] RSP: 0018:ffffc90000ff7698 EFLAGS: 00010282
[ 24.963376] RAX: ffff888028397010 RBX: ffff88800c26e630 RCX: 0000000000000058
[ 24.963458] RDX: ffff88800c26f844 RSI: 0000000000000006 RDI: ffff888028397010
[ 24.963538] RBP: ffff88800ea72f00 R08: 18b873fbab2b964c R09: be06b38235f3c63c
[ 24.963622] R10: 18b873fbab2b964c R11: be06b38235f3c63c R12: 0000000000000001
[ 24.963705] R13: ffff88800c26f84c R14: ffff8880063f0ff8 R15: ffff88800c26e644
[ 24.963788] FS: 00007effcea327c0(0000) GS:ffff88807dc00000(0000) knlGS:0000000000000000
[ 24.963871] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[ 24.963941] CR2: ffff88800c223200 CR3: 0000000000eaa2000 CR4: 00000000000006b0
[ 24.964018] note: wpa_supplicant[391] exited with irqs disabled
```

Fixes: d1369e515efe ("wifi: mt76: connac: introduce mt76_connac_mcu_sta_wed_update utility routine")
Signed-off-by: Lorenzo Bianconi <lorenzo@kernel.org>
Acked-by: Felix Fietkau <nbd@nbd.name>
Signed-off-by: Kalle Valo <kvalo@kernel.org>
Link: <https://lore.kernel.org/r/c42168429453474213fa8244bf4b069de4531f40.1678124335.git.lorenzo@kernel.org>
Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

```
-rw-r--r-- drivers/net/wireless/mediatek/mt76/mt76_connac_mcu.c 3
```

1 files changed, 3 insertions, 0 deletions

```
diff --git a/drivers/net/wireless/mediatek/mt76/mt76_connac_mcu.c b/drivers/net/wireless/mediatek/mt76/mt76_connac_mcu.c
index 5a047e630860f3..d106cbfc387c8b 100644
```

```
--- a/drivers/net/wireless/mediatek/mt76/mt76_connac_mcu.c
```

```
+++ b/drivers/net/wireless/mediatek/mt76/mt76_connac_mcu.c
```

```
@@ -1221,6 +1221,9 @@ EXPORT_SYMBOL_GPL(mt76_connac_mcu_sta_ba_tlv);
```

```
int mt76_connac_mcu_sta_wed_update(struct mt76_dev *dev, struct sk_buff *skb)
{
+     if (!mt76_is_mmio(dev))
+         return 0;
+
     if (!mtk_wed_device_active(&dev->mmio.wed))
         return 0;
```