author	Remi Pommarel <repk@triplefau.lt>	2025-03-24 17:28:21 +0100
committer	Johannes Berg <johannes.berg@intel.com>	2025-04-02 10:48:23 +0200
commit	378677eb8f44621ecc9ce659f7af61e5baa94d81 (patch)	
tree	b83493e51ae80e2c9eddd62168c184baacc868c5	
parent	a104042e2bf6528199adb6ca901efe7b60c2c27f (diff)	
download	linux-378677eb8f44621ecc9ce659f7af61e5baa94d81.tar.gz	

wifi: mac80211: Purge vif txq in ieee80211_do_stop()

After ieee80211_do_stop() SKB from vif's txq could still be processed.
Indeed another concurrent vif schedule_and_wake_txq call could cause
those packets to be dequeued (see ieee80211_handle_wake_tx_queue())
without checking the sdata current state.

Because vif.drv_priv is now cleared in this function, this could lead to
driver crash.

For example in ath12k, ahvif is store in vif.drv_priv. Thus if
ath12k_mac_op_tx() is called after ieee80211_do_stop(), ahvif->ah can be
NULL, leading the ath12k_warn(ahvif->ah,...) call in this function to
trigger the NULL deref below.

```
  Unable to handle kernel paging request at virtual address dfffffc000000001
  KASAN: null-ptr-deref in range [0x0000000000000008-0x000000000000000f]
  batman_adv: bat0: Interface deactivated: brbh1337
  Mem abort info:
    ESR = 0x0000000096000004
    EC = 0x25: DABT (current EL), IL = 32 bits
    SET = 0, FnV = 0
    EA = 0, S1PTW = 0
    FSC = 0x04: level 0 translation fault
  Data abort info:
    ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000
    CM = 0, WnR = 0, TnD = 0, TagAccess = 0
    GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0
  [dfffffc000000001] address between user and kernel address ranges
  Internal error: Oops: 0000000096000004 [#1] SMP
  CPU: 1 UID: 0 PID: 978 Comm: lbd Not tainted 6.13.0-g633f875b8f1e #114
  Hardware name: HW (DT)
  pstate: 10000005 (nzcV daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--)
  pc : ath12k_mac_op_tx+0x6cc/0x29b8 [ath12k]
  lr : ath12k_mac_op_tx+0x174/0x29b8 [ath12k]
  sp : ffffffc086ace450
  x29: ffffffc086ace450 x28: 0000000000000000 x27: 1ffffff810d59ca4
  x26: ffffff801d05f7c0 x25: 0000000000000000 x24: 000000004000001e
  x23: ffffff8009ce4926 x22: ffffff801f9c0800 x21: ffffff801d05f7f0
  x20: ffffff8034a19f40 x19: 0000000000000000 x18: ffffff801f9c0958
  x17: ffffff800bc0a504 x16: dfffffc000000000 x15: ffffffc086ace4f8
  x14: ffffff801d05f83c x13: 0000000000000000 x12: ffffffb003a0bf03
  x11: 0000000000000000 x10: ffffffb003a0bf02 x9 : ffffff8034a19f40
  x8 : ffffff801d05f818 x7 : 1ffffff0069433dc x6 : ffffff8034a19ee0
  x5 : ffffff801d05f7f0 x4 : 0000000000000000 x3 : 0000000000000001
  x2 : 0000000000000000 x1 : dfffffc000000000 x0 : 0000000000000008
  Call trace:
   ath12k_mac_op_tx+0x6cc/0x29b8 [ath12k] (P)
```

```
   ieee80211_handle_wake_tx_queue+0x16c/0x260
   ieee80211_queue_skb+0xeec/0x1d20
   ieee80211_tx+0x200/0x2c8
   ieee80211_xmit+0x22c/0x338
   __ieee80211_subif_start_xmit+0x7e8/0xc60
   ieee80211_subif_start_xmit+0xc4/0xee0
   __ieee80211_subif_start_xmit_8023.isra.0+0x854/0x17a0
   ieee80211_subif_start_xmit_8023+0x124/0x488
   dev_hard_start_xmit+0x160/0x5a8
   __dev_queue_xmit+0x6f8/0x3120
   br_dev_queue_push_xmit+0x120/0x4a8
   __br_forward+0xe4/0x2b0
   deliver_clone+0x5c/0xd0
   br_flood+0x398/0x580
   br_dev_xmit+0x454/0x9f8
   dev_hard_start_xmit+0x160/0x5a8
   __dev_queue_xmit+0x6f8/0x3120
   ip6_finish_output2+0xc28/0x1b60
   __ip6_finish_output+0x38c/0x638
   ip6_output+0x1b4/0x338
   ip6_local_out+0x7c/0xa8
   ip6_send_skb+0x7c/0x1b0
   ip6_push_pending_frames+0x94/0xd0
   rawv6_sendmsg+0x1a98/0x2898
   inet_sendmsg+0x94/0xe0
   __sys_sendto+0x1e4/0x308
   __arm64_sys_sendto+0xc4/0x140
   do_el0_svc+0x110/0x280
   el0_svc+0x20/0x60
   el0t_64_sync_handler+0x104/0x138
   el0t_64_sync+0x154/0x158

To avoid that, empty vif's txq at ieee80211_do_stop() so no packet could
be dequeued after ieee80211_do_stop() (new packets cannot be queued
because SDATA_STATE_RUNNING is cleared at this point).

Fixes: ba8c3d6f16a1 ("mac80211: add an intermediate software queue implementation")
Signed-off-by: Remi Pommarel <repk@triplefau.lt>
Link: https://patch.msgid.link/ff7849e268562456274213c0476e09481a48f489.1742833382.git.repk@triplefau.lt
Signed-off-by: Johannes Berg <johannes.berg@intel.com>
```

Diffstat

-rw-r--r-- net/mac80211/iface.c 3

1 files changed, 3 insertions, 0 deletions

```
diff --git a/net/mac80211/iface.c b/net/mac80211/iface.c
index b0423046028c57..183b63235000a7 100644
--- a/net/mac80211/iface.c
+++ b/net/mac80211/iface.c
@@ -659,6 +659,9 @@ static void ieee80211_do_stop(struct ieee80211_sub_if_data *sdata, bool going_do
        if (sdata->vif.type == NL80211_IFTYPE_AP_VLAN)
                ieee80211_txq_remove_vlan(local, sdata);

+       if (sdata->vif.txq)
+               ieee80211_txq_purge(sdata->local, to_txq_info(sdata->vif.txq));
+
        sdata->bss = NULL;

        if (local->open_count == 0)
```