batman-adv - Bug #404

KCSAN: data-race in batadv_tt_local_add / batadv_tt_local_add

11/08/2019 03:41 PM - Sven Eckelmann

Status:	New	**Start date:**	11/08/2019
Priority:	Normal	**Due date:**	
Assignee:	Antonio Quartulli	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

The new KCSAN (concurrency sanitizer) reported a problem with the TT code:
https://lists.open-mesh.org/mailman3/hyperkitty/list/b.a.t.m.a.n@lists.open-mesh.org/message/Z44URGZT3NKZP5273KQEMW27WHGNJEUP/

```
Hello,

syzbot found the following crash on:

HEAD commit:    05f22368 x86, kcsan: Enable KCSAN for x86
git tree:       https://github.com/google/ktsan.git kcsan
console output: https://syzkaller.appspot.com/x/log.txt?x=1195a0d4e00000
kernel config:  https://syzkaller.appspot.com/x/.config?x=87d111955f40591f
dashboard link: https://syzkaller.appspot.com/bug?extid=1d5dadec56d9e87f0aac
compiler:       gcc (GCC) 9.0.0 20181231 (experimental)

Unfortunately, I don't have any reproducer for this crash yet.

IMPORTANT: if you fix the bug, please add the following tag to the commit:
Reported-by: syzbot+1d5dadec56d9e87f0aac@syzkaller.appspotmail.com

==================================================================
BUG: KCSAN: data-race in batadv_tt_local_add / batadv_tt_local_add

write to 0xffff8880a8e19698 of 2 bytes by task 10064 on cpu 0:
  batadv_tt_local_add+0x21b/0x1020 net/batman-adv/translation-table.c:799
  batadv_interface_tx+0x398/0xae0 net/batman-adv/soft-interface.c:249
  __netdev_start_xmit include/linux/netdevice.h:4420 [inline]
  netdev_start_xmit include/linux/netdevice.h:4434 [inline]
  xmit_one net/core/dev.c:3280 [inline]
  dev_hard_start_xmit+0xef/0x430 net/core/dev.c:3296
  __dev_queue_xmit+0x14c9/0x1b60 net/core/dev.c:3873
  dev_queue_xmit+0x21/0x30 net/core/dev.c:3906
  __bpf_tx_skb net/core/filter.c:2060 [inline]
  __bpf_redirect_common net/core/filter.c:2099 [inline]
  __bpf_redirect+0x4b4/0x710 net/core/filter.c:2106
  ____bpf_clone_redirect net/core/filter.c:2139 [inline]
  bpf_clone_redirect+0x1a5/0x1f0 net/core/filter.c:2111
  bpf_prog_bb15b996d00816f9+0x71c/0x1000
  bpf_test_run+0x1c3/0x490 net/bpf/test_run.c:44
  bpf_prog_test_run_skb+0x4da/0x840 net/bpf/test_run.c:310
  bpf_prog_test_run kernel/bpf/syscall.c:2108 [inline]
  __do_sys_bpf+0x1664/0x2b90 kernel/bpf/syscall.c:2884
  __se_sys_bpf kernel/bpf/syscall.c:2825 [inline]
  __x64_sys_bpf+0x4c/0x60 kernel/bpf/syscall.c:2825
  do_syscall_64+0xcc/0x370 arch/x86/entry/common.c:290
  entry_SYSCALL_64_after_hwframe+0x44/0xa9

read to 0xffff8880a8e19698 of 2 bytes by task 9969 on cpu 1:
  batadv_tt_local_add+0x3d1/0x1020 net/batman-adv/translation-table.c:801
  batadv_interface_tx+0x398/0xae0 net/batman-adv/soft-interface.c:249
  __netdev_start_xmit include/linux/netdevice.h:4420 [inline]
  netdev_start_xmit include/linux/netdevice.h:4434 [inline]
```

```
  xmit_one net/core/dev.c:3280 [inline]
  dev_hard_start_xmit+0xef/0x430 net/core/dev.c:3296
  __dev_queue_xmit+0x14c9/0x1b60 net/core/dev.c:3873
  dev_queue_xmit+0x21/0x30 net/core/dev.c:3906
  __bpf_tx_skb net/core/filter.c:2060 [inline]
  __bpf_redirect_common net/core/filter.c:2099 [inline]
  __bpf_redirect+0x4b4/0x710 net/core/filter.c:2106
  ____bpf_clone_redirect net/core/filter.c:2139 [inline]
  bpf_clone_redirect+0x1a5/0x1f0 net/core/filter.c:2111
  bpf_prog_bb15b996d00816f9+0x312/0x1000
  bpf_test_run+0x1c3/0x490 net/bpf/test_run.c:44
  bpf_prog_test_run_skb+0x4da/0x840 net/bpf/test_run.c:310
  bpf_prog_test_run kernel/bpf/syscall.c:2108 [inline]
  __do_sys_bpf+0x1664/0x2b90 kernel/bpf/syscall.c:2884
  __se_sys_bpf kernel/bpf/syscall.c:2825 [inline]
  __x64_sys_bpf+0x4c/0x60 kernel/bpf/syscall.c:2825
  do_syscall_64+0xcc/0x370 arch/x86/entry/common.c:290

Reported by Kernel Concurrency Sanitizer on:
CPU: 1 PID: 9969 Comm: syz-executor.2 Not tainted 5.4.0-rc3+ #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS
Google 01/01/2011
==================================================================

---
This bug is generated by a bot. It may contain errors.
See https://goo.gl/tpsmEJ for more information about syzbot.
syzbot engineers can be reached at syzkaller@googlegroups.com.

syzbot will keep track of this bug report. See:
https://goo.gl/tpsmEJ#status for how to communicate with syzbot.
```

History

#1 - 11/08/2019 03:45 PM - Sven Eckelmann

The relevant code is:

```
    if (batadv_is_wifi_hardif(in_hardif))
        tt_local->common.flags |= BATADV_TT_CLIENT_WIFI;
    else
        tt_local->common.flags &= ~BATADV_TT_CLIENT_WIFI;
```

So removing and adding this flag is not correctly protected with a method which prevents data races.

#2 - 05/27/2020 09:24 PM - Sven Eckelmann

- Description updated