batman-adv - Bug #412

general protection fault in batadv_hardif_get_by_netdev

07/22/2020 08:55 PM - Sven Eckelmann

Status:	New	**Start date:**	07/22/2020
Priority:	Normal	**Due date:**	
Assignee:	batman-adv developers	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

```
Hello,

syzbot found the following crash on:

HEAD commit:    0aea6d5c Merge tag 'for-linus-5.8b-rc5-tag' of git://git.k..
git tree:       upstream
console output: https://syzkaller.appspot.com/x/log.txt?x=1596004f100000
kernel config:  https://syzkaller.appspot.com/x/.config?x=66ad203c2bb6d8b
dashboard link: https://syzkaller.appspot.com/bug?extid=4a2d01c2df834fe6e86d
compiler:       gcc (GCC) 10.1.0-syz 20200507
userspace arch: i386

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+4a2d01c2df834fe6e86d@syzkaller.appspotmail.com

netlink: 24 bytes leftover after parsing attributes in process `syz-executor.4'.
general protection fault, probably for non-canonical address 0xdfffc0000000003: 0000 [#1] PREEMPT
 SMP KASAN
KASAN: null-ptr-deref in range [0x0000000000000018-0x000000000000001f]
CPU: 1 PID: 11316 Comm: syz-executor.4 Not tainted 5.8.0-rc4-syzkaller #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011
RIP: 0010:batadv_hardif_get_by_netdev+0x14c/0x400 net/batman-adv/hard-interface.c:72
Code: 18 00 0f 85 92 02 00 00 4d 8b 24 24 49 81 fc e0 29 4f 8d 0f 84 b4 01 00 00 e8 00 01 ab f9 49
 8d 7c 24 18 48 89 f8 48 c1 e8 03 <80> 3c 18 00 0f 85 73 02 00 00 4d 39 6c 24 18 75 b7 e8 de 00 ab
 f9
RSP: 0018:ffffc900171aeca8 EFLAGS: 00010206
RAX: 0000000000000003 RBX: dfffc0000000000 RCX: ffffc90011a8c000
RDX: 0000000000040000 RSI: ffffffff87c8b900 RDI: 0000000000000018
RBP: ffff88802afd4000 R08: 0000000000000000 R09: ffffffff8c593a27
R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000000
R13: ffff88802afd4000 R14: 0000000000000000 R15: ffffffff8aa441c0
FS:  0000000000000000(0000) GS:ffff8880ae700000(0063) knlGS:00000000f5d6db40
CS:  0010 DS: 002b ES: 002b CR0: 0000000080050033
CR2: 000055feecf1dcd8 CR3: 0000000027b29000 CR4: 00000000001426e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
Call Trace:
 batadv_hard_if_event+0x62/0x12f0 net/batman-adv/hard-interface.c:1031
 notifier_call_chain+0xb5/0x200 kernel/notifier.c:83
 call_netdevice_notifiers_info+0xb5/0x130 net/core/dev.c:2027
 call_netdevice_notifiers_extack net/core/dev.c:2039 [inline]
 call_netdevice_notifiers net/core/dev.c:2053 [inline]
 register_netdevice+0xa52/0x1540 net/core/dev.c:9509
 veth_newlink+0x405/0xa00 drivers/net/veth.c:1366
 __rtnl_newlink+0x1090/0x1730 net/core/rtnetlink.c:3339
 rtnl_newlink+0x64/0xa0 net/core/rtnetlink.c:3397
 rtnetlink_rcv_msg+0x44e/0xad0 net/core/rtnetlink.c:5460
 netlink_rcv_skb+0x15a/0x430 net/netlink/af_netlink.c:2469
 netlink_unicast_kernel net/netlink/af_netlink.c:1303 [inline]
```

```
 netlink_unicast+0x533/0x7d0 net/netlink/af_netlink.c:1329
 netlink_sendmsg+0x856/0xd90 net/netlink/af_netlink.c:1918
 sock_sendmsg_nosec net/socket.c:652 [inline]
 sock_sendmsg+0xcf/0x120 net/socket.c:672
 ____sys_sendmsg+0x6e8/0x810 net/socket.c:2352
 ___sys_sendmsg+0xf3/0x170 net/socket.c:2406
 __sys_sendmsg+0xe5/0x1b0 net/socket.c:2439
 do_syscall_32_irqs_on+0x3f/0x60 arch/x86/entry/common.c:428
 __do_fast_syscall_32 arch/x86/entry/common.c:475 [inline]
 do_fast_syscall_32+0x7f/0x120 arch/x86/entry/common.c:503
 entry_SYSENTER_compat_after_hwframe+0x4d/0x5c
RIP: 0023:0xf7f72569
Code: Bad RIP value.
RSP: 002b:00000000f5d6d0cc EFLAGS: 00000296 ORIG_RAX: 0000000000000172
RAX: ffffffffffffffda RBX: 0000000000000007 RCX: 0000000020000040
RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000
RBP: 0000000000000000 R08: 0000000000000000 R09: 0000000000000000
R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000000
R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000
Modules linked in:
```

See also:

- https://lists.open-mesh.org/mailman3/hyperkitty/list/b.a.t.m.a.n@lists.open-mesh.org/message/EPSHQY7VW75OYEEU2NAWCIEN7XUM2AKJ/