batman-adv - Bug #411

general protection fault in batadv_iv_ogm_schedule_buff (2)

07/07/2020 10:04 PM - Sven Eckelmann

Status:	New	**Start date:**	07/07/2020
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:    7cc2a8ea Merge tag 'block-5.8-2020-07-01' of git://git.ker..
git tree:       upstream
console output: https://syzkaller.appspot.com/x/log.txt?x=130b828f100000
kernel config:  https://syzkaller.appspot.com/x/.config?x=7be693511b29b338
dashboard link: https://syzkaller.appspot.com/bug?extid=2eeeb5ad0766b57394d8
compiler:       gcc (GCC) 10.1.0-syz 20200507

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+2eeeb5ad0766b57394d8@syzkaller.appspotmail.com

general protection fault, probably for non-canonical address 0xdffffc000000000e: 0000 [#1] PREEMPT
 SMP KASAN
KASAN: null-ptr-deref in range [0x0000000000000070-0x0000000000000077]
CPU: 1 PID: 9126 Comm: kworker/u4:9 Not tainted 5.8.0-rc3-syzkaller #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011
Workqueue: bat_events batadv_iv_send_outstanding_bat_ogm_packet
RIP: 0010:batadv_iv_ogm_schedule_buff+0xd1e/0x1410 net/batman-adv/bat_iv_ogm.c:843
Code: 80 3c 28 00 0f 85 ee 05 00 00 4d 8b 3f 49 81 ff e0 e9 4e 8d 0f 84 dd 02 00 00 e8 bd 80 ae f9
 49 8d 7f 70 48 89 f8 48 c1 e8 03 <42> 80 3c 28 00 0f 85 af 06 00 00 48 8b 44 24 08 49 8b 6f 70 80
 38
RSP: 0018:ffffc90004e97b98 EFLAGS: 00010202
RAX: 000000000000000e RBX: ffff8880a7471800 RCX: ffffffff87c5394d
RDX: ffff88804cf02380 RSI: ffffffff87c536a3 RDI: 0000000000000070
RBP: 0000000000077000 R08: 0000000000000001 R09: ffff8880a875a02b
R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000007
R13: dffffc0000000000 R14: ffff888051ad4c40 R15: 0000000000000000
FS:  0000000000000000(0000) GS:ffff8880ae700000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 0000000000400200 CR3: 0000000061cac000 CR4: 00000000001426e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
Call Trace:
 batadv_iv_ogm_schedule net/batman-adv/bat_iv_ogm.c:869 [inline]
 batadv_iv_ogm_schedule net/batman-adv/bat_iv_ogm.c:862 [inline]
 batadv_iv_send_outstanding_bat_ogm_packet+0x5c8/0x800 net/batman-adv/bat_iv_ogm.c:1722
 process_one_work+0x94c/0x1670 kernel/workqueue.c:2269
 worker_thread+0x64c/0x1120 kernel/workqueue.c:2415
 kthread+0x3b5/0x4a0 kernel/kthread.c:291
 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:293
Modules linked in:
---[ end trace f5c5eda032070cd1 ]---
RIP: 0010:batadv_iv_ogm_schedule_buff+0xd1e/0x1410 net/batman-adv/bat_iv_ogm.c:843
Code: 80 3c 28 00 0f 85 ee 05 00 00 4d 8b 3f 49 81 ff e0 e9 4e 8d 0f 84 dd 02 00 00 e8 bd 80 ae f9
 49 8d 7f 70 48 89 f8 48 c1 e8 03 <42> 80 3c 28 00 0f 85 af 06 00 00 48 8b 44 24 08 49 8b 6f 70 80
 38
```

```
RSP: 0018:ffffc90004e97b98 EFLAGS: 00010202
RAX: 000000000000000e RBX: ffff8880a7471800 RCX: ffffffff87c5394d
RDX: ffff88804cf02380 RSI: ffffffff87c536a3 RDI: 0000000000000070
RBP: 0000000000077000 R08: 0000000000000001 R09: ffff8880a875a02b
R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000007
R13: dfffffc0000000000 R14: ffff888051ad4c40 R15: 0000000000000000
FS:  0000000000000000(0000) GS:ffff8880ae700000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 0000000000400200 CR3: 000000009480d000 CR4: 00000000001426e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
```

See also

- https://lists.open-mesh.org/mailman3/hyperkitty/list/b.a.t.m.a.n@lists.open-mesh.org/thread/XBVBFSLNCT73H2AELGD4Y7HRMZU5C4EX/
- https://groups.google.com/forum/#!msg/syzkaller-lts-bugs/L9X3uBxeRLQ/w0SggdN7AAAJ
- https://lists.open-mesh.org/mailman3/hyperkitty/list/b.a.t.m.a.n@lists.open-mesh.org/thread/JFEOUTPZP7GTO73PX7I47JJX2XX2EX4Y/

History

#1 - 07/07/2020 11:00 PM - Sven Eckelmann

- Description updated

#2 - 09/10/2020 11:46 AM - Sven Eckelmann

- Description updated