batman-adv - Bug #407

Invalid pointer during OGM schedule

02/08/2020 08:43 PM - Sven Eckelmann

Status:	Closed	**Start date:**	02/08/2020
Priority:	Normal	**Due date:**	
Assignee:	batman-adv developers	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	2020.0		

Description

syzbot found a crash in batadv_iv_send_outstanding_bat_ogm_packet when interfaces are removed from the bat0

```
Hello,

syzbot found the following crash on:

HEAD commit:    f7571657 Merge tag 'fuse-fixes-5.6-rc1' of git://git.kerne..
git tree:       upstream
console output: https://syzkaller.appspot.com/x/log.txt?x=12dddbbee00000
kernel config:  https://syzkaller.appspot.com/x/.config?x=7f1d914a74bd6ddc
dashboard link: https://syzkaller.appspot.com/bug?extid=ac36b6a33c28a491e929
compiler:       clang version 10.0.0 (https://github.com/llvm/llvm-project/ c2443155a0fb245c8f17f2
c1c72b6ea391e86e81)

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+ac36b6a33c28a491e929@syzkaller.appspotmail.com

general protection fault, probably for non-canonical address 0xdfffc0000000002: 0000 [#1] PREEMPT
 SMP KASAN
KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017]
CPU: 0 PID: 465 Comm: kworker/u4:5 Not tainted 5.5.0-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 net/batman-adv/bat_iv_ogm.c:814 [inline]
RIP: 0010:batadv_iv_ogm_schedule+0x220/0xf00 net/batman-adv/bat_iv_ogm.c:865
Code: e8 35 ef bf f9 4c 89 ad 60 ff ff ff 4d 8b 75 00 66 41 c1 c7 08 49 8d 5e 16 48 89 d8 48 c1 e8
 03 49 bd 00 00 00 00 00 fc ff df <42> 8a 04 28 84 c0 0f 85 e0 0b 00 00 66 44 89 3b 4c 89 a5 78 ff
 ff
RSP: 0018:ffffc90002887b78 EFLAGS: 00010203
RAX: 0000000000000002 RBX: 0000000000000016 RCX: 1ffff11012580611
RDX: 0000000000000000 RSI: ffff8880a80449b0 RDI: 0000000000000282
RBP: ffffc90002887c38 R08: dfffffc0000000000 R09: fffffbfff12d3605
R10: fffffbfff12d3605 R11: 0000000000000000 R12: ffff888092c03000
R13: dfffffc0000000000 R14: 0000000000000000 R15: 0000000000000000
FS:  0000000000000000(0000) GS:ffff8880aea00000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 000000000075bfd4 CR3: 0000000090ab0000 CR4: 00000000001406f0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
Call Trace:
 batadv_iv_send_outstanding_bat_ogm_packet+0x664/0x770 net/batman-adv/bat_iv_ogm.c:1718
 process_one_work+0x7f5/0x10f0 kernel/workqueue.c:2264
 worker_thread+0xbbc/0x1630 kernel/workqueue.c:2410
 kthread+0x332/0x350 kernel/kthread.c:255
 ret_from_fork+0x24/0x30 arch/x86/entry/entry_64.S:352
Modules linked in:
---[ end trace eddf69e5e4c9f596 ]---
RIP: 0010:batadv_iv_ogm_schedule_buff net/batman-adv/bat_iv_ogm.c:814 [inline]
RIP: 0010:batadv_iv_ogm_schedule+0x220/0xf00 net/batman-adv/bat_iv_ogm.c:865
Code: e8 35 ef bf f9 4c 89 ad 60 ff ff ff 4d 8b 75 00 66 41 c1 c7 08 49 8d 5e 16 48 89 d8 48 c1 e8
```

```
 03 49 bd 00 00 00 00 00 fc ff df <42> 8a 04 28 84 c0 0f 85 e0 0b 00 00 66 44 89 3b 4c 89 a5 78 ff
 ff
RSP: 0018:ffffc90002887b78 EFLAGS: 00010203
RAX: 0000000000000002 RBX: 0000000000000016 RCX: 1ffff11012580611
RDX: 0000000000000000 RSI: ffff8880a80449b0 RDI: 0000000000000282
RBP: ffffc90002887c38 R08: dfffffc0000000000 R09: fffffbfff12d3605
R10: fffffbfff12d3605 R11: 0000000000000000 R12: ffff888092c03000
R13: dfffffc0000000000 R14: 0000000000000000 R15: 0000000000000000
FS:  0000000000000000(0000) GS:ffff8880aea00000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 000000000075bfd4 CR3: 000000009c67b000 CR4: 00000000001406f0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400

---
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.
```

The relevant code section is:

```
803         if (hard_iface == primary_if) {
 804                 /* tt changes have to be committed before the tvlv data is
 805                  * appended as it may alter the tt tvlv container
 806                  */
 807                 batadv_tt_local_commit_changes(bat_priv);
 808                 tvlv_len = batadv_tvlv_container_ogm_append(bat_priv, ogm_buff,
 809                                                             ogm_buff_len,
 810                                                             BATADV_OGM_HLEN);
 811         }
 812
 813         batadv_ogm_packet = (struct batadv_ogm_packet *)(*ogm_buff);
 814         batadv_ogm_packet->tvlv_len = htons(tvlv_len);
 815
 816         /* change sequence number to network order */
 817         seqno = (u32)atomic_read(&hard_iface->bat_iv.ogm_seqno);
 818         batadv_ogm_packet->seqno = htonl(seqno);
 819         atomic_inc(&hard_iface->bat_iv.ogm_seqno);
 820
 821         batadv_iv_ogm_slide_own_bcast_window(hard_iface)
```

Could this be some kind of use after free?

History

#1 - 02/16/2020 01:22 PM - Sven Eckelmann

See also

- https://lists.open-mesh.org/mailman3/hyperkitty/list/b.a.t.m.a.n@lists.open-mesh.org/message/BMQIC77OQDUAQEBI5RLCDBDZQYBIWF4I/
- https://lists.open-mesh.org/mailman3/hyperkitty/list/b.a.t.m.a.n@lists.open-mesh.org/message/CZRJVSVYR5VRQYQOGQHC5ST6OAOMQ24H/

#2 - 02/17/2020 05:46 PM - Sven Eckelmann

- % Done changed from 0 to 100

- Target version set to 2020.0

- Status changed from New to Resolved

The untested [1] patch was submitted as https://patchwork.open-mesh.org/project/b.a.t.m.a.n./patch/20200217141641.26999-1-sven@narfation.org/

[1] there is currently no good reproducer for this bug

#3 - 03/04/2020 01:25 PM - Sven Eckelmann

- Status changed from Resolved to Closed