batman-adv - Bug #292

sporadic crashes with v2016.2

07/26/2016 09:56 PM - Lars B

Status:	Closed	**Start date:**	07/26/2016
Priority:	Normal	**Due date:**	
Assignee:	Lars B	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2016.3		

Description

With batman v2016.2 we have issue with sporadic crashes on our gateways. The machines are crashing approximately every 6 days.

Setup:
Debian 8
Virtual KVM Machine (1CPU, 2GB Memory)
Kernel 4.5.0-0.bpo.2-amd64
10 Batman Instances

Traces are attached. A kernel dump is also available if useful.

History

#1 - 07/26/2016 11:22 PM - Sven Eckelmann

We don't have your module builds and therefore can only interpret the oops in a very limited way. Maybe the function in your build looks like this:

```
0000000000000170 <batadv_neigh_node_release>:
     170:       e8 00 00 00 00          callq  175 <batadv_neigh_node_release+0x5>
     175:       41 55                   push   %r13
     177:       41 54                   push   %r12
     179:       4c 8d 6f b8             lea    -0x48(%rdi),%r13
     17d:       55                      push   %rbp
     17e:       53                      push   %rbx
     17f:       48 89 fd                mov    %rdi,%rbp
     182:       48 8b 47 c8             mov    -0x38(%rdi),%rax
     186:       48 8b 80 c8 00 00 00    mov    0xc8(%rax),%rax
     18d:       4c 8b a0 f0 01 00 00    mov    0x1f0(%rax),%r12
     194:       48 8b 47 d8             mov    -0x28(%rdi),%rax
     198:       48 85 c0                test   %rax,%rax
     19b:       74 16                   je     1b3 <batadv_neigh_node_release+0x43>
     19d:       48 8b 18                mov    (%rax),%rbx
     1a0:       48 8d 78 34             lea    0x34(%rax),%rdi
     1a4:       f0 83 68 34 01          lock subl $0x1,0x34(%rax)
     1a9:       74 49                   je     1f4 <batadv_neigh_node_release+0x84>
     1ab:       48 85 db                test   %rbx,%rbx
     1ae:       48 89 d8                mov    %rbx,%rax
     1b1:       75 ea                   jne    19d <batadv_neigh_node_release+0x2d>
     1b3:       48 8b 45 f8             mov    -0x8(%rbp),%rax
     1b7:       48 8d 78 28             lea    0x28(%rax),%rdi
     1bb:       f0 83 68 28 01          lock subl $0x1,0x28(%rax)
     1c0:       74 39                   je     1fb <batadv_neigh_node_release+0x8b>
     1c2:       49 8b 44 24 70          mov    0x70(%r12),%rax
     1c7:       48 85 c0                test   %rax,%rax
     1ca:       74 05                   je     1d1 <batadv_neigh_node_release+0x61>
     1cc:       4c 89 ef                mov    %r13,%rdi
     1cf:       ff d0                   callq  *%rax
     1d1:       48 8b 45 e8             mov    -0x18(%rbp),%rax
     1d5:       48 8d 78 30             lea    0x30(%rax),%rdi
     1d9:       f0 83 68 30 01          lock subl $0x1,0x30(%rax)
     1de:       74 22                   je     202 <batadv_neigh_node_release+0x92>
     1e0:       5b                      pop    %rbx
     1e1:       48 8d 7d 08             lea    0x8(%rbp),%rdi
     1e5:       be 50 00 00 00          mov    $0x50,%esi
     1ea:       5d                      pop    %rbp
     1eb:       41 5c                   pop    %r12
     1ed:       41 5d                   pop    %r13
```

```
    1ef:       e9 00 00 00 00          jmpq   1f4 <batadv_neigh_node_release+0x84>
    1f4:       e8 b7 fe ff ff          callq  b0 <batadv_neigh_ifinfo_release>
    1f9:       eb b0                   jmp    1ab <batadv_neigh_node_release+0x3b>
    1fb:       e8 f0 fe ff ff          callq  f0 <batadv_hardif_neigh_release>
    200:       eb c0                   jmp    1c2 <batadv_neigh_node_release+0x52>
    202:       e8 00 00 00 00          callq  207 <batadv_neigh_node_release+0x97>
    207:       eb d7                   jmp    1e0 <batadv_neigh_node_release+0x70>
    209:       0f 1f 80 00 00 00 00    nopl   0x0(%rax)
```

This would mean that the IP is at following line:

```
    18d:       4c 8b a0 f0 01 00 00    mov    0x1f0(%rax),%r12
```

This should be the neigh_node->orig_node->bat_priv->bat_algo_ops in batadv_neigh_node_release

```
    neigh_node = container_of(ref, struct batadv_neigh_node, refcount);
    bao = neigh_node->orig_node->bat_priv->bat_algo_ops;
```

Annotated version to understand how I came to the conclusion:

```
0000000000000170 <batadv_neigh_node_release>:
    170:       e8 00 00 00 00          callq  175 <batadv_neigh_node_release+0x5>
    175:       41 55                   push   %r13
    177:       41 54                   push   %r12
    179:       4c 8d 6f b8             lea    -0x48(%rdi),%r13 <--- from kref to neigh_node
    17d:       55                      push   %rbp
    17e:       53                      push   %rbx
    17f:       48 89 fd                mov    %rdi,%rbp
    182:       48 8b 47 c8             mov    -0x38(%rdi),%rax <--- neigh_node->orig_node
    186:       48 8b 80 c8 00 00 00    mov    0xc8(%rax),%rax <--- neigh_node->orig_node->bat_priv
    18d:       4c 8b a0 f0 01 00 00    mov    0x1f0(%rax),%r12 <--- neigh_node->orig_node->bat_priv->bat_algo
_ops
```

This code was also removed in https://git.open-mesh.org/batman-adv.git/commit/ecd23344249c8ef2c535cb86fef15ac7c33aabdf

Everything looks like the messed up backpointers without reference counters and any other protection. Most likely, orig_node was not valid anymore when the neigh_node is free'd.

Now to things which you could do:

Could you upgrade in the meantime to the maint branch (v2016.2 + fixes)? Everything up to 12c771df4b9c200ea0b53886c3a0939a16097c02 (current state of the maint branch) are fixes which exist in batman-adv since a longer time. Please also try to apply the patch https://git.open-mesh.org/batman-adv.git/patch/ecd23344249c8ef2c535cb86fef15ac7c33aabdf. I have prepared everything for you in the branch ecsv/issue-292

If it doesn't help then we should create a KASAN version of your kernel and let it run in your kvm setup. Then please compile the module with make EXTRA_CFLAGS="-fno-inline -O1 -fno-optimize-sibling-calls" KERNELPATH=/home/to/your/kasan/kernel/headers V=1. This should give us a lot more of information when the crash happens

#2 - 07/27/2016 08:26 AM - Sven Eckelmann

- Assignee set to Lars B

- Status changed from New to Feedback

#3 - 07/27/2016 09:40 PM - Lars B

Thanks for your fast reply!

I upgraded to branch ecsv/issue-292 and will report feedback in the next days.

#4 - 08/08/2016 09:16 PM - Lars B

The issue is solved with the branch! :-)
No crashes after upgrading

#5 - 08/08/2016 09:34 PM - Sven Eckelmann

- Status changed from Feedback to Resolved

Thanks a lot for testing and reporting back. The change will be in the next release (it is currently in the next branch which should be released in the near future as v2016.3).

#6 - 09/01/2016 06:30 PM - Sven Eckelmann

- Status changed from Resolved to Closed

v2016.3 was just released

#7 - 02/11/2017 08:34 AM - Sven Eckelmann

- Target version set to 2016.3

Files

dmesg.201607161458	129 KB	07/26/2016	Lars B
dmesg.201607221551	127 KB	07/26/2016	Lars B