batman-adv - Bug #147

Null pointer dereference in orig_hash_del_if()

03/08/2011 06:43 PM - Linus Lüssing

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	2011.2.0		

Description

When doing a rmmod of the batman-adv kernel module, the system freezes. I didn't have this bug with just two interfaces added in batman-adv, however with four ones, it happens every time.

I also need at least two VMs connected to each other to produce this bug. I'm doing the starting and stopping of batman-adv nearly at the same time with parallel-ssh on all VMs.

This bug is present in both v2011.0.0 and svn r1955.

See attachment for full call trace and OS information.

PS: The locking dependancy info seems to be another issue (see ticket #145).

History

#1 - 03/08/2011 07:14 PM - Linus Lüssing

Ok, with some printk()s, I could track it down to this line:
https://git.open-mesh.org/?p=batman-adv.git;a=blob;f=originator.c;h=0b9133022d2dd58f3f91d55940667ede6dab9e50;hb=refs/heads/master#l544

#2 - 03/08/2011 11:34 PM - Linus Lüssing

That's what happens on rmmod with the four interfaces:

```
[   70.772525] batman_adv: bat0: Removing interface: eth1
[   70.778656] λλλ orig_node_del_if: del_if_num: 0, chunk_size: 8, max_if_num: 3, +dst: 0, +src: 8, num: 24
[   71.101053] λλλ orig_node_del_if: del_if_num: 0, chunk_size: 8, max_if_num: 3, +dst: 0, +src: 8, num: 24
[   71.422060] λλλ orig_node_del_if: del_if_num: 0, chunk_size: 8, max_if_num: 3, +dst: 0, +src: 8, num: 24
[   71.701043] batman_adv: bat0: Interface deactivated: eth2
[   71.703874] batman_adv: bat0: Removing interface: eth2
[   71.707313] λλλ orig_node_del_if: del_if_num: 1, chunk_size: 8, max_if_num: 2, +dst: 8, +src: 16, num: 8
[   72.001061] λλλ orig_node_del_if: del_if_num: 1, chunk_size: 8, max_if_num: 2, +dst: 8, +src: 16, num: 8
[   72.318055] λλλ orig_node_del_if: del_if_num: 1, chunk_size: 8, max_if_num: 2, +dst: 8, +src: 16, num: 8
[   72.643099] batman_adv: bat0: Interface deactivated: eth3
[   72.645943] batman_adv: bat0: Removing interface: eth3
[   72.696057] λλλ orig_node_del_if: del_if_num: 2, chunk_size: 8, max_if_num: 1, +dst: 16, +src: 24, num: -8
[   72.849028] BUG: unable to handle kernel
```

- *+dst*: memcpy's dest offset (del_if_num * chunk_size)
- *+src*: memcpy's src offset ((del_if_num + 1) * chunk_size)
- *num*: number of bytes to copy (max_if_num - del_if_num) * chunk_size)
  of this memcpy

When an interface is deleted, all following interfaces' if_num should be decreased by one, and not only the buffers should be resized. So after for instance "batman_adv: bat0: Removing interface: eth2", the del_if_num should still be 0, and not 1.

The tricky part is to reduce the "if_num"s by one and doing the resizing in one atomic operation... Looks like we need to introduce a spinlock for that?

Furthermore: Check, if there's a cast missing here:

Instead of:

```
orig_node->bcast_own + ((del_if_num + 1) * chunk_size),
```

do

```
(char*)orig_node->bcast_own + ((del_if_num + 1) * chunk_size),
```

or

```
orig_node->bcast_own + ((del_if_num + 1) * NUM_WORDS),
```

#3 - 05/07/2011 05:20 AM - Linus Lüssing

- % Done changed from 0 to 100

- Assignee deleted (Anonymous)

- Status changed from New to Resolved

Fixed in 7e95055

#4 - 05/07/2011 05:27 AM - Linus Lüssing

- Status changed from Resolved to Closed

#5 - 02/11/2017 09:31 AM - Sven Eckelmann

- Target version set to 2011.2.0

Files

2011-03-08-null-pointer-dereference.log	33.7 KB	03/08/2011	Linus Lüssing