batman-adv - Bug #146

unable to handle kernel NULL pointer dereference

03/03/2011 03:16 AM - Linus Lüssing

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:	Linus Lüssing	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2011.1.0		

Description

On commit f39fe6f230e4cbf2b04e659b056ea62a652578a0 from the master branch, I get the following crash on my laptop (Linux Linus-Debian 2.6.32-5-amd64 #1 SMP Sat Sep 18 03:26:20 UTC 2010 x86_64 GNU/Linux):

```
[  286.097842] batman_adv: B.A.T.M.A.N. advanced devel v0.2-319-gf39fe6f (compatibility version 12
) loaded
[  290.737762] batman_adv: bat0: Adding interface: br0
[  290.737771] batman_adv: bat0: The MTU of interface br0 is too small (1500) to handle the transp
ort of batman-adv packets. Packets going over this interface will be fragmented on layer2 which co
uld impact the performance. Setting the MTU to 1527 would solve the problem.
[  290.737783] batman_adv: bat0: Interface activated: br0
[  312.262887] batman_adv: bat0: Interface deactivated: br0
[  312.262895] batman_adv: bat0: Removing interface: br0
[  312.297134] BUG: unable to handle kernel NULL pointer dereference at 0000000000000010
[  312.297147] IP: [<ffffffffa002aaa6>] orig_hash_add_if+0x129/0x144 [batman_adv]
[  312.297168] PGD 37a6b067 PUD 6dc40067 PMD 0
[  312.297178] Oops: 0000 [#1] SMP
[  312.297185] last sysfs file: /sys/devices/virtual/net/br0/batman_adv/mesh_iface
[  312.297192] CPU 1
[  312.297196] Modules linked in: batman_adv acpi_cpufreq cpufreq_conservative cpufreq_userspace c
pufreq_stats tun parport_pc ppdev lp parport sco bnep rfcomm l2cap crc16 cpufreq_powersave binfmt_
misc fuse nfsd exportfs nfs lockd fscache nfs_acl auth_rpcgss sunrpc ppp_generic slhc bridge stp c
oretemp firewire_sbp2 loop snd_hda_codec_realtek arc4 snd_hda_intel ecb snd_hda_codec iwlagn snd_h
wdep iwlcore uvcvideo snd_pcm_oss snd_mixer_oss snd_pcm videodev snd_seq_midi mac80211 snd_rawmidi
 v4l1_compat snd_seq_midi_event snd_seq v4l2_compat_ioctl32 cfg80211 nvidia(P) acer_wmi snd_timer
btusb snd_seq_device bluetooth snd rfkill i2c_i801 i2c_core pcspkr soundcore psmouse video snd_pag
e_alloc output battery processor button ac serio_raw evdev wmi ext3 jbd mbcache sha256_generic aes
_x86_64 aes_generic cbc dm_crypt dm_mod sg sr_mod usb_storage cdrom sd_mod crc_t10dif ata_generic
tg3 thermal ahci uhci_hcd ata_piix sdhci_pci sdhci ricoh_mmc firewire_ohci firewire_core crc_itu_t
 mmc_core led_class libphy thermal_sys ehci_hcd libata scsi_mod usbcore nls_base [last unloaded: s
csi_wait_scan]
[  312.297400] Pid: 3033, comm: sh Tainted: P           2.6.32-5-amd64 #1 ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
[  312.297406] RIP: 0010:[<ffffffffa002aaa6>]  [<ffffffffa002aaa6>] orig_hash_add_if+0x129/0x144 [
batman_adv]
[  312.297425] RSP: 0000:ffff88007e11fe08  EFLAGS: 00010202
[  312.297427] RAX: 0000000000000008 RBX: ffff88007d5d4640 RCX: 0000000000038000
[  312.297429] RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffff88007e09ccc0
[  312.297432] RBP: ffff88007e09ccc0 R08: ffff8800374c67e8 R09: ffffffff8144df10
[  312.297434] R10: ffff88007e05dc00 R11: dead000000200200 R12: ffff88007f0a4680
[  312.297436] R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000
[  312.297439] FS:  0000000000000000(0000) GS:ffff880001900000(0063) knlGS:00000000f76256c0
[  312.297441] CS:  0010 DS: 002b ES: 002b CR0: 000000008005003b
[  312.297444] CR2: 0000000000000010 CR3: 000000006dc13000 CR4: 00000000000006e0
[  312.297446] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[  312.297448] DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400
[  312.297451] Process sh (pid: 3033, threadinfo ffff88007e11e000, task ffff88007e877100)
[  312.297453] Stack:
[  312.297454]  ffff8800374c67e8 ffff88007eee3000 0000000000000000 0000000000000008
[  312.297458] <0> 0000000000000001 ffff88007d5d4640 ffff88007e09ccc0 ffff88007f0a4680
[  312.297462] <0> 0000000000000020 ffff88007f0a4000 ffffffff81483960 ffffffffa00299b0
[  312.297466] Call Trace:
[  312.297471]  [<ffffffffa00299b0>] ? hardif_enable_interface+0x141/0x289 [batman_adv]
[  312.297476]  [<ffffffffa0027bd4>] ? store_mesh_iface+0x11c/0x14c [batman_adv]
```

```
[  312.297482]  [<ffffffff8113c1c1>] ? sysfs_write_file+0xd0/0x107
[  312.297486]  [<ffffffff810ecdee>] ? vfs_write+0xa9/0x102
[  312.297489]  [<ffffffff810ecf03>] ? sys_write+0x45/0x6e
[  312.297494]  [<ffffffff81036070>] ? sysenter_dispatch+0x7/0x2e
[  312.297496] Code: a2 0b e1 49 89 5c 24 20 31 db 48 8b 7c 24 08 e8 97 b4 2c e1 ff c3 0f 85 41 ff
 ff ff b8 f4 ff ff ff eb 14 41 ff c5 48 8b 54 24 10 <44> 3b 6a 10 0f 8c 14 ff ff ff 31 c0 48 83 c4
 28 5b 5d 41 5c 41
[  312.297525] RIP  [<ffffffffa002aaa6>] orig_hash_add_if+0x129/0x144 [batman_adv]
[  312.297531]  RSP <ffff88007e11fe08>
[  312.297532] CR2: 0000000000000010
[  312.297535] ---[ end trace 752f4ae6f2526ec1 ]---
[  331.562603] device lo entered promiscuous mode
[  358.707599] ioctl32(pimd:2431): Unknown cmd fd(3) cmd(000089e1){t:ffffff89;sz:0} arg(ffd0230c)
on socket:r7845
[  365.861488] batman_adv: lo: Removing interface: br0
[  365.861498] dev_remove_pack: ffff88007e09cd08 not found.
[  365.877111] BUG: unable to handle kernel NULL pointer dereference at 0000000000000010
[  365.877124] IP: [<ffffffffa002a916>] orig_hash_del_if+0x179/0x1e0 [batman_adv]
[  365.877145] PGD 6dd57067 PUD 6dd5d067 PMD 0
[  365.877155] Oops: 0000 [#2] SMP
[  365.877162] last sysfs file: /sys/devices/virtual/net/br0/batman_adv/mesh_iface
[  365.877169] CPU 1
[  365.877174] Modules linked in: batman_adv acpi_cpufreq cpufreq_conservative cpufreq_userspace c
pufreq_stats tun parport_pc ppdev lp parport sco bnep rfcomm l2cap crc16 cpufreq_powersave binfmt_
misc fuse nfsd exportfs nfs lockd fscache nfs_acl auth_rpcgss sunrpc ppp_generic slhc bridge stp c
oretemp firewire_sbp2 loop snd_hda_codec_realtek arc4 snd_hda_intel ecb snd_hda_codec iwlagn snd_h
wdep iwlcore uvcvideo snd_pcm_oss snd_mixer_oss snd_pcm videodev snd_seq_midi mac80211 snd_rawmidi
 v4l1_compat snd_seq_midi_event snd_seq v4l2_compat_ioctl32 cfg80211 nvidia(P) acer_wmi snd_timer
btusb snd_seq_device bluetooth snd rfkill i2c_i801 i2c_core pcspkr soundcore psmouse video snd_pag
e_alloc output battery processor button ac serio_raw evdev wmi ext3 jbd mbcache sha256_generic aes
_x86_64 aes_generic cbc dm_crypt dm_mod sg sr_mod usb_storage cdrom sd_mod crc_t10dif ata_generic
tg3 thermal ahci uhci_hcd ata_piix sdhci_pci sdhci ricoh_mmc firewire_ohci firewire_core crc_itu_t
 mmc_core led_class libphy thermal_sys ehci_hcd libata scsi_mod usbcore nls_base [last unloaded: s
csi_wait_scan]
[  365.877378] Pid: 3050, comm: sh Tainted: P      D    2.6.32-5-amd64 #1 ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
[  365.877384] RIP: 0010:[<ffffffffa002a916>]  [<ffffffffa002a916>] orig_hash_del_if+0x179/0x1e0 [
batman_adv]
[  365.877401] RSP: 0018:ffff88007e0c1e08  EFLAGS: 00010292
[  365.877407] RAX: 0000000000000000 RBX: ffff88007f0a4000 RCX: dead000000200200
[  365.877414] RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffff88007e09ccc0
[  365.877420] RBP: ffff88007e09ccc0 R08: ffff88007e0c0000 R09: ffff880001915780
[  365.877427] R10: ffff88007d2a2a00 R11: 0000001c99674047 R12: ffff88007f0a4680
[  365.877433] R13: 00000000ffffff02 R14: 0000000000000000 R15: ffff88007e09ccc0
[  365.877441] FS:  0000000000000000(0000) GS:ffff880001900000(0063) knlGS:00000000f76256c0
[  365.877448] CS:  0010 DS: 002b ES: 002b CR0: 000000008005003b
[  365.877454] CR2: 0000000000000010 CR3: 000000006dca1000 CR4: 00000000000006e0
[  365.877461] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[  365.877467] DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400
[  365.877475] Process sh (pid: 3050, threadinfo ffff88007e0c0000, task ffff88007e1baa60)
[  365.877480] Stack:
[  365.877483]  ffff88007e09ccc0 ffff88007f0a4680 00000000ffffff02 0000000000000000
[  365.877493] <0> 0000000081483960 0000000000000000 0000000000000000 ffff88007f0a4000
[  365.877503] <0> ffff88007e09ccc0 ffff88007f0a4680 00000000ffffff02 0000000000000005
[  365.877515] Call Trace:
[  365.877530]  [<ffffffffa0029347>] ? hardif_disable_interface+0x6a/0x189 [batman_adv]
[  365.877542]  [<ffffffffa0027bc4>] ? store_mesh_iface+0x10c/0x14c [batman_adv]
[  365.877556]  [<ffffffff8113c1c1>] ? sysfs_write_file+0xd0/0x107
[  365.877567]  [<ffffffff810ecdee>] ? vfs_write+0xa9/0x102
[  365.877575]  [<ffffffff810ecf03>] ? sys_write+0x45/0x6e
[  365.877586]  [<ffffffff81036070>] ? sysenter_dispatch+0x7/0x2e
[  365.877591] Code: 89 5d 20 31 db 48 8b 7c 24 10 e8 2c b6 2c e1 ff c3 0f 85 fc fe ff ff b8 f4 ff
 ff ff eb 65 ff 44 24 24 48 8b 54 24 18 8b 44 24 24 <3b> 42 10 0f 8c c9 fe ff ff 48 8b 15 0a 91 00
 00 eb 2e 80 7a 12
[  365.877673] RIP  [<ffffffffa002a916>] orig_hash_del_if+0x179/0x1e0 [batman_adv]
[  365.877688]  RSP <ffff88007e0c1e08>
[  365.877692] CR2: 0000000000000010
[  365.877699] ---[ end trace 752f4ae6f2526ec2 ]---
```

History

#1 - 03/03/2011 03:29 AM - Linus Lüssing

Ok, this can easily reproduced with the following stupid configuration attempt:

```
echo lo > /sys/class/net/br0/batman_adv/mesh_iface
insmod batman-adv.ko
```

I'll look into it.

#2 - 03/03/2011 03:30 AM - Linus Lüssing

insmod batman-adv.ko
echo lo > /sys/class/net/br0/batman_adv/mesh_iface

#3 - 03/06/2011 02:52 AM - Linus Lüssing

- Status changed from New to Closed

fixed in r1955

#4 - 02/11/2017 09:34 AM - Sven Eckelmann

- Target version set to 2011.1.0

- Description updated