batman-adv - Bug #135

redzone problem (rev 1517)

12/30/2009 01:50 AM - Simon Wunderlich

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2011.0.0		

Description

i had 2 qemu openwrt instances, set the orig interval to 50 and adding (not existant) interfaces as stresstest with this script:

```
for i in $(seq 0 100); do echo eth$i > /proc/net/batman-adv/interfaces ; done
```

i've repeated this a few times and cleared the interface list again with "echo > /proc/net/batman-adv/interfaces".

suddenly, i got this error message:

```
=============================================================================
BUG kmalloc-16: Redzone overwritten
-----------------------------------------------------------------------------

INFO: 0xc13762d0-0xc13762d3. First byte 0x98 instead of 0xcc
INFO: Allocated in get_orig_node+0xeb/0x1c9 [batman_adv] age=1 cpu=0 pid=515
INFO: Freed in hardif_add_interface+0x23d/0x3e0 [batman_adv] age=321 cpu=0 pid=515
INFO: Slab 0xc1975ec0 objects=64 used=12 fp=0xc1376300 flags=0x400000c3
INFO: Object 0xc13762c0 @offset=704 fp=0x826ec601

Bytes b4 0xc13762b0:  03 02 00 00 1f 0d 02 00 5a 5a 5a 5a 5a 5a 5a 5a ........ZZZZZZZZ
  Object 0xc13762c0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
 Redzone 0xc13762d0:  98 99 99 99                                     ....
 Padding 0xc13762f8:  5a 5a 5a 5a 5a 5a 5a 5a                         ZZZZZZZZ
Pid: 515, comm: ash Not tainted 2.6.31.1 #53
Call Trace:
 [<c1376010>] ? mtrr_trim_uncached_memory+0x270/0x530
 [<c1376010>] ? mtrr_trim_uncached_memory+0x270/0x530
 [<c10a1f12>] print_trailer+0x122/0x130
 [<c13762c0>] ? mtrr_trim_uncached_memory+0x520/0x530
 [<c13762c0>] ? mtrr_trim_uncached_memory+0x520/0x530
 [<c13762d4>] ? amd_init_mtrr+0x4/0x20
 [<c13762d3>] ? amd_init_mtrr+0x3/0x20
 [<c13762d0>] ? amd_init_mtrr+0x0/0x20
 [<c10a1fc2>] check_bytes_and_report+0xa2/0xd0
 [<c13762d0>] ? amd_init_mtrr+0x0/0x20
 [<c13762d3>] ? amd_init_mtrr+0x3/0x20
 [<c13762c0>] ? mtrr_trim_uncached_memory+0x520/0x530
 [<c13762d0>] ? amd_init_mtrr+0x0/0x20
 [<c13762c0>] ? mtrr_trim_uncached_memory+0x520/0x530
 [<c10a22a4>] check_object+0x54/0x200
 [<c13762d0>] ? amd_init_mtrr+0x0/0x20
 [<c13762c0>] ? mtrr_trim_uncached_memory+0x520/0x530
 [<c10a29c7>] +slab_free+0x177/0x2d0
 [<c10a2ef9>] kfree+0x119/0x150
 [<c2af557e>] ? hardif_add_interface+0x1fe/0x3e0 [batman_adv]
 [<c13762c0>] ? mtrr_trim_uncached_memory+0x520/0x530
 [<c2af557e>] ? hardif_add_interface+0x1fe/0x3e0 [batman_adv]
 [<c13762d8>] ? amd_init_mtrr+0x8/0x20
 [<c2af557e>] hardif_add_interface+0x1fe/0x3e0 [batman_adv]
 [<c2af0035>] setup_procfs+0x7b5/0xcf0 [batman_adv]
```

```
 [<c2aeffb0>] ? setup_procfs+0x730/0xcf0 [batman_adv]
 [<c2aeff10>] ? setup_procfs+0x690/0xcf0 [batman_adv]
 [<c10e1d0f>] proc_reg_write+0x6f/0x90
 [<c10aa6fe>] vfs_write+0x9e/0x120
 [<c10e1ca0>] ? proc_reg_write+0x0/0x90
 [<c10aac52>] sys_write+0x42/0x70
 [<c1003259>] syscall_call+0x7/0xb
FIX kmalloc-16: Restoring 0xc13762d0-0xc13762d3=0xcc
```

History

#1 - 03/26/2011 09:24 PM - Anonymous

- Assignee deleted (Anonymous)

- Category set to 2

#2 - 11/01/2011 11:37 AM - Simon Wunderlich

- Status changed from New to Closed

the implementation changed from proc to sys filesystems, allowing only existent interfaces to be added.

therefore, this bug is obsolete.

#3 - 02/11/2017 09:40 AM - Sven Eckelmann

- Target version set to 2011.0.0