batman-adv - Bug #420

KMSAN: uninit-value in batadv_nc_worker

10/01/2020 01:49 PM - Sven Eckelmann

Status:	New	**Start date:**	10/01/2020
Priority:	Normal	**Due date:**	
Assignee:	Martin Hundebøll	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

```
Hello,

syzbot found the following issue on:

HEAD commit:    5edb1df2 kmsan: drop the _nosanitize string functions
git tree:       https://github.com/google/kmsan.git master
console output: https://syzkaller.appspot.com/x/log.txt?x=10cc55a7900000
kernel config:  https://syzkaller.appspot.com/x/.config?x=4991d22eb136035c
dashboard link: https://syzkaller.appspot.com/bug?extid=da9194708de785081f11
compiler:       clang version 10.0.0 (https://github.com/llvm/llvm-project/ c2443155a0fb245c8f17f2
c1c72b6ea391e86e81)

Unfortunately, I don't have any reproducer for this issue yet.

IMPORTANT: if you fix the issue, please add the following tag to the commit:
Reported-by: syzbot+da9194708de785081f11@syzkaller.appspotmail.com

==================================================
BUG: KMSAN: uninit-value in batadv_nc_purge_orig_hash net/batman-adv/network-coding.c:408 [inline]
BUG: KMSAN: uninit-value in batadv_nc_worker+0x1c0/0x1d70 net/batman-adv/network-coding.c:718
CPU: 0 PID: 7 Comm: kworker/u4:0 Not tainted 5.9.0-rc4-syzkaller #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011
Workqueue: bat_events batadv_nc_worker
Call Trace:
 __dump_stack lib/dump_stack.c:77 [inline]
 dump_stack+0x21c/0x280 lib/dump_stack.c:118
 kmsan_report+0xf7/0x1e0 mm/kmsan/kmsan_report.c:122
 __msan_warning+0x58/0xa0 mm/kmsan/kmsan_instr.c:201
 batadv_nc_purge_orig_hash net/batman-adv/network-coding.c:408 [inline]
 batadv_nc_worker+0x1c0/0x1d70 net/batman-adv/network-coding.c:718
 process_one_work+0x1688/0x2140 kernel/workqueue.c:2269
 worker_thread+0x10bc/0x2730 kernel/workqueue.c:2415
 kthread+0x551/0x590 kernel/kthread.c:293
 ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:294

Uninit was created at:
 kmsan_save_stack_with_flags mm/kmsan/kmsan.c:143 [inline]
 kmsan_internal_poison_shadow+0x66/0xd0 mm/kmsan/kmsan.c:126
 kmsan_slab_alloc+0x8a/0xe0 mm/kmsan/kmsan_hooks.c:80
 slab_alloc_node mm/slub.c:2907 [inline]
 slab_alloc mm/slub.c:2916 [inline]
 __kmalloc+0x2bb/0x4b0 mm/slub.c:3982
 kmalloc_array+0x90/0x140 include/linux/slab.h:594
 batadv_hash_new+0x129/0x530 net/batman-adv/hash.c:52
 batadv_originator_init+0x9b/0x370 net/batman-adv/originator.c:211
 batadv_mesh_init+0x4dc/0x9d0 net/batman-adv/main.c:204
 batadv_softif_init_late+0x6d8/0xa30 net/batman-adv/soft-interface.c:857
 register_netdevice+0xbbc/0x37d0 net/core/dev.c:9760
 __rtnl_newlink net/core/rtnetlink.c:3454 [inline]
 rtnl_newlink+0x2e77/0x3ed0 net/core/rtnetlink.c:3500
 rtnetlink_rcv_msg+0x142b/0x18c0 net/core/rtnetlink.c:5563
```

```
 netlink_rcv_skb+0x6d7/0x7e0 net/netlink/af_netlink.c:2470
 rtnetlink_rcv+0x50/0x60 net/core/rtnetlink.c:5581
 netlink_unicast_kernel net/netlink/af_netlink.c:1304 [inline]
 netlink_unicast+0x11c8/0x1490 net/netlink/af_netlink.c:1330
 netlink_sendmsg+0x173a/0x1840 net/netlink/af_netlink.c:1919
 sock_sendmsg_nosec net/socket.c:651 [inline]
 sock_sendmsg net/socket.c:671 [inline]
 __sys_sendto+0x9dc/0xc80 net/socket.c:1992
 __do_sys_sendto net/socket.c:2004 [inline]
 __se_sys_sendto+0x107/0x130 net/socket.c:2000
 __x64_sys_sendto+0x6e/0x90 net/socket.c:2000
 do_syscall_64+0x9f/0x140 arch/x86/entry/common.c:48
 entry_SYSCALL_64_after_hwframe+0x44/0xa9
=====================================================
```

See also:

- https://lists.open-mesh.org/mailman3/hyperkitty/list/b.a.t.m.a.n@lists.open-mesh.org/message/TFZFXLUH5GYL5NCR4CCAANDB2IPUPIYU/
- https://lists.open-mesh.org/mailman3/hyperkitty/list/b.a.t.m.a.n@lists.open-mesh.org/message/HZN6NKEIY6JRCOFXE3O7OGPPUXGBVC3U/