Messages in this thread

- *First message in thread*
- *syzbot*
- **syzbot**

Date Sat, 15 Feb 2020 07:33:13 -0800
Subject Re: kernel panic: stack is corrupted in vhost_net_ioctl
From syzbot <>

```
syzbot has found a reproducer for the following crash on:

HEAD commit:    2019fc96 Merge git://git.kernel.org/pub/scm/linux/kernel/g..
git tree:       upstream
console output: https://syzkaller.appspot.com/x/log.txt?x=1677602de00000
kernel config:  https://syzkaller.appspot.com/x/.config?x=6780df5a5f208964
dashboard link: https://syzkaller.appspot.com/bug?extid=f2a62d07a5198c819c7b
compiler:       clang version 10.0.0 (https://github.com/llvm/llvm-project/ c2443155a0fb245c8f17f2c1c72b6ea391e86e81)
syz repro:      https://syzkaller.appspot.com/x/repro.syz?x=16dcd87ee00000
C reproducer:   https://syzkaller.appspot.com/x/repro.c?x=1135fa31e00000

Bisection is inconclusive: the bug happens on the oldest tested release.

bisection log:  https://syzkaller.appspot.com/x/bisect.txt?x=13204371e00000
final crash:    https://syzkaller.appspot.com/x/report.txt?x=10a04371e00000
console output: https://syzkaller.appspot.com/x/log.txt?x=17204371e00000

IMPORTANT: if you fix the bug, please add the following tag to the commit:
Reported-by: syzbot+f2a62d07a5198c819c7b@syzkaller.appspotmail.com

Kernel panic - not syncing: stack-protector: Kernel stack is corrupted in: vhost_net_ioctl+0x1d83/0x1db0 drivers/vhost/net.c:366
CPU: 0 PID: 8673 Comm: syz-executor239 Not tainted 5.6.0-rc1-syzkaller #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011
Call Trace:
 __dump_stack lib/dump_stack.c:77 [inline]
 dump_stack+0x1fb/0x318 lib/dump_stack.c:118
 panic+0x264/0x7a9 kernel/panic.c:221
 __stack_chk_fail+0x1f/0x20 kernel/panic.c:667
 vhost_net_ioctl+0x1d83/0x1db0 drivers/vhost/net.c:366
 vfs_ioctl fs/ioctl.c:47 [inline]
 ksys_ioctl fs/ioctl.c:763 [inline]
 __do_sys_ioctl fs/ioctl.c:772 [inline]
 __se_sys_ioctl+0x113/0x190 fs/ioctl.c:770
 __x64_sys_ioctl+0x7b/0x90 fs/ioctl.c:770
 do_syscall_64+0xf7/0x1c0 arch/x86/entry/common.c:294
 entry_SYSCALL_64_after_hwframe+0x49/0xbe
RIP: 0033:0x440259
Code: 18 89 d0 c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 0f 83 fb 13 fc ff c3 66 2e 0f 1f 84 00 00 00 00
RSP: 002b:00007ffdeb5890b8 EFLAGS: 00000246 ORIG_RAX: 0000000000000010
RAX: ffffffffffffffda RBX: 00000000004002c8 RCX: 0000000000440259
RDX: 0000000020f1dff8 RSI: 000000004008af30 RDI: 0000000000000003
RBP: 00000000006ca018 R08: 00000000004002c8 R09: 00000000004002c8
R10: 00000000004002c8 R11: 0000000000000246 R12: 0000000000401ae0
R13: 0000000000401b70 R14: 0000000000000000 R15: 0000000000000000
Kernel Offset: disabled
Rebooting in 86400 seconds..
```