



author Wang Yufen <wangyufen@huawei.com> 2022-11-02 17:41:19 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-16 09:58:16 +0100
commit [d7569302a7a52a9305d2fb054df908ff985553bb](#) (patch)
tree [d903b060a44fec812a2473252cf012230d67347](#)
parent [430d1f4964dddcc44be00fee4d1af0e728bf60bc](#) (diff)
download [linux-d7569302a7a52a9305d2fb054df908ff985553bb.tar.gz](#)

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

net: tun: Fix memory leaks of napi_get_frags

[Upstream commit 1118b2049d77ca0b505775fc1a8d1909cf19a7ec]

kmemleak reports after running test_progs:

unreferenced object 0xffff8881b1672dc0 (size 232):

comm "test_progs", pid 394388, jiffies 4354712116 (age 841.975s)

hex dump (first 32 bytes):

```
e0 84 d7 a8 81 88 ff ff 80 2c 67 b1 81 88 ff ff .....g.....
00 40 c5 9b 81 88 ff ff 00 00 00 00 00 00 00 00 .@.....
```

backtrace:

```
[<00000000c8f01748>] napi_skb_cache_get+0xd4/0x150
[<00000000041c7fc09>] __napi_build_skb+0x15/0x50
[<000000000431c7079>] __napi_alloc_skb+0x26e/0x540
[<0000000003ecfa30e>] napi_get_frags+0x59/0x140
[<00000000099b2199e>] tun_get_user+0x183d/0x3bb0 [tun]
[<0000000008a5adef0>] tun_chr_write_iter+0xc0/0x1b1 [tun]
[<00000000049993ff4>] do_iter_readv_writev+0x19f/0x320
[<0000000008f338ea2>] do_iter_write+0x135/0x630
[<0000000008a3377a4>] vfs_writev+0x12e/0x440
[<000000000a6b5639a>] do_writev+0x104/0x280
[<000000000ccf065d8>] do_syscall_64+0x3b/0x90
[<000000000d776e329>] entry_SYSCALL_64_after_hwframe+0x63/0xcd
```

The issue occurs in the following scenarios:

```
tun_get_user()
  napi_gro_frags()
    napi_frags_finish()
      case GRO_NORMAL:
        gro_normal_one()
          list_add_tail(&skb->list, &napi->rx_list);
          <-- While napi->rx_count < READ_ONCE(gro_normal_batch),
          <-- gro_normal_list() is not called, napi->rx_list is not empty
          <-- not ask to complete the gro work, will cause memory leaks in
          <-- following tun_napi_del()
        ...
      tun_napi_del()
        netif_napi_del()
          __netif_napi_del()
            <-- &napi->rx_list is not empty, which caused memory leaks
```

To fix, add `napi_complete()` after `napi_gro_frags()`.

Fixes: 90e33d459407 ("tun: enable napi_gro_frags() for TUN/TAP driver")
Signed-off-by: Wang Yufen <wangyufen@huawei.com>
Reviewed-by: Eric Dumazet <edumazet@google.com>
Signed-off-by: David S. Miller <davem@davemloft.net>
Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

-rw-r--r-- drivers/net/tun.c 1

1 files changed, 1 insertions, 0 deletions

```
diff --git a/drivers/net/tun.c b/drivers/net/tun.c
index 9909f430d723ff..4e77b269ef0a1f 100644
--- a/drivers/net/tun.c
+++ b/drivers/net/tun.c
@@ -1959,6 +1959,7 @@ drop:
```

```
        local_bh_disable();
        napi_gro_frags(&tfile->napi);
+       napi_complete(&tfile->napi);
        local_bh_enable();
        mutex_unlock(&tfile->napi_mutex);
    } else if (tfile->napi_enabled) {
```