



author Xin Long <lu cien.xin@gmail.com> 2022-11-04 16:48:53 -0400
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-16 10:03:56 +0100
commit [6cee2c60bd168279852ac7dbe54c2b70d1028644](#) (patch)
tree [6ed9f89c18eae40e5b7cdf4b8debe4cecfbf8663](#)
parent [a54309860d7677ec2bb38c1c9961d7623a5319f4](#) (diff)
download [linux-6cee2c60bd168279852ac7dbe54c2b70d1028644.tar.gz](#)

diff options

context: 3 ▼
space: include ▼
mode: unified ▼

tipc: fix the msg->req tlv len check in tipc_nl_compat_name_table_dump_header

[Upstream commit [1c075b192fe41030457cd4a5f7dea730412bca40](#)]

This is a follow-up for commit [974cb0e3e7c9](#) ("tipc: fix uninit-value in tipc_nl_compat_name_table_dump") where it should have type casted sizeof(..) to int to work when TLV_GET_DATA_LEN() returns a negative value.

syzbot reported a call trace because of it:

```
BUG: KMSAN: uninit-value in ...
tipc_nl_compat_name_table_dump+0x841/0xea0 net/tipc/netlink_compat.c:934
__tipc_nl_compat_dumpit+0xab2/0x1320 net/tipc/netlink_compat.c:238
tipc_nl_compat_dumpit+0x991/0xb50 net/tipc/netlink_compat.c:321
tipc_nl_compat_rcv_msg_doit net/netlink/genetlink.c:731 [inline]
genl_family_rcv_msg net/netlink/genetlink.c:775 [inline]
genl_rcv_msg+0x103f/0x1260 net/netlink/genetlink.c:792
netlink_rcv_skb+0x3a5/0x6c0 net/netlink/af_netlink.c:2501
genl_rcv+0x3c/0x50 net/netlink/genetlink.c:803
netlink_unicast_kernel net/netlink/af_netlink.c:1319 [inline]
netlink_unicast+0xf3b/0x1270 net/netlink/af_netlink.c:1345
netlink_sendmsg+0x1288/0x1440 net/netlink/af_netlink.c:1921
sock_sendmsg_nosec net/socket.c:714 [inline]
sock_sendmsg net/socket.c:734 [inline]
```

Reported-by: [syzbot+e5dbaaa238680ce206ea@syzkaller.appspotmail.com](#)

Fixes: [974cb0e3e7c9](#) ("tipc: fix uninit-value in tipc_nl_compat_name_table_dump")

Signed-off-by: Xin Long <lu cien.xin@gmail.com>

Link: <https://lore.kernel.org/r/ccd6a7ea801b15aec092c3b532a883b4c5708695.1667594933.git.lucien.xin@gmail.com>

Signed-off-by: Jakub Kicinski <kuba@kernel.org>

Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

```
-rw-r--r-- net/tipc/netlink_compat.c 2
```

1 files changed, 1 insertions, 1 deletions

diff --git a/net/tipc/netlink_compat.c b/net/tipc/netlink_compat.c

index 0749df80454d4f..ce00f271ca6b2b 100644

--- a/net/tipc/netlink_compat.c

+++ b/net/tipc/netlink_compat.c

```
@@ -880,7 +880,7 @@ static int tipc_nl_compat_name_table_dump_header(struct tipc_nl_compat_msg *msg)
    };
```

```
    ntq = (struct tipc_name_table_query *)TLV_DATA(msg->req);
```

```
-    if (TLV_GET_DATA_LEN(msg->req) < sizeof(struct tipc_name_table_query))
```

```
+    if (TLV_GET_DATA_LEN(msg->req) < (int)sizeof(struct tipc_name_table_query))
```

```
        return -EINVAL;
```

depth = ntohl(ntq->depth);