



author Zhengchao Shao <shaozhengchao@huawei.com> 2022-10-28 16:56:50 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-25 17:42:05 +0100
commit [afab4655750fcb3fca359bc7d7214e3d634cdf9c](#) (patch)
tree [c6d5237bfad66465b71846d4188a7bbf7938d0d5](#)
parent [58cd7fdc8c1e6c7873acc08f190069fed88d1c12](#) (diff)
download [linux-afab4655750fcb3fca359bc7d7214e3d634cdf9c.tar.gz](#)

diff options

context: ▼
space: ▼
mode: ▼

can: af_can: fix NULL pointer dereference in can_rx_register()

[Upstream commit 8aa59e355949442c408408c2d836e561794c40a1]

It causes NULL pointer dereference when testing as following:

- (a) use `syscall(__NR_socket, 0x10ul, 3ul, 0)` to create netlink socket.
- (b) use `syscall(__NR_sendmsg, ...)` to create bond link device and vxcan link device, and bind vxcan device to bond device (can also use `ifenslave` command to bind vxcan device to bond device).
- (c) use `syscall(__NR_socket, 0x1dul, 3ul, 1)` to create CAN socket.
- (d) use `syscall(__NR_bind, ...)` to bind the bond device to CAN socket.

The bond device invokes the can-raw protocol registration interface to receive CAN packets. However, `ml_priv` is not allocated to the dev, `dev_rcv_lists` is assigned to NULL in `can_rx_register()`. In this case, it will occur the NULL pointer dereference issue.

The following is the stack information:

BUG: kernel NULL pointer dereference, address: 0000000000000008

PGD 122a4067 P4D 122a4067 PUD 1223c067 PMD 0

Oops: 0000 [#1] PREEMPT SMP

RIP: 0010:can_rx_register+0x12d/0x1e0

Call Trace:

<TASK>

raw_enable_filters+0x8d/0x120

raw_enable_allfilters+0x3b/0x130

raw_bind+0x118/0x4f0

__sys_bind+0x163/0x1a0

__x64_sys_bind+0x1e/0x30

do_syscall_64+0x35/0x80

entry_SYSCALL_64_after_hwframe+0x63/0xcd

</TASK>

Fixes: 4e096a18867a ("net: introduce CAN specific pointer in the struct net_device")

Signed-off-by: Zhengchao Shao <shaozhengchao@huawei.com>

Reviewed-by: Marc Kleine-Budde <mkl@pengutronix.de>

Link: <https://lore.kernel.org/all/20221028085650.170470-1-shaozhengchao@huawei.com>

Signed-off-by: Marc Kleine-Budde <mkl@pengutronix.de>

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

Diffstat

-rw-r--r-- net/can/af_can.c 2

1 files changed, 1 insertions, 1 deletions

```
diff --git a/net/can/af_can.c b/net/can/af_can.c
index c758a12ffe4611..f7dc68cd86e4b6 100644
--- a/net/can/af_can.c
+++ b/net/can/af_can.c
@@ -450,7 +450,7 @@ int can_rx_register(struct net *net, struct net_device *dev, canid_t can_id,

    /* insert new receiver (dev,canid,mask) -> (func,data) */

-    if (dev && dev->type != ARPHRD_CAN)
+    if (dev && (dev->type != ARPHRD_CAN || !can_get_ml_priv(dev)))
        return -ENODEV;

    if (dev && !net_eq(net, dev_net(dev)))
```