author	Zhengchao Shao <shaozhengchao@huawei.com>	2022-10-28 16:56:50 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2022-11-16 09:58:19 +0100
commit	261178a1c2623077d62e374a75c195e6c99a6f05 (patch)	
tree	2842ecdc1628c91117c63c79620d89bd5a2b7e54	
parent	2acb2779b147decd300c117683d5a32ce61c75d6 (diff)	
download	linux-261178a1c2623077d62e374a75c195e6c99a6f05.tar.gz	

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 <sashal@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 cce2af10eb3eab..4ddefa6a3e055f 100644
--- a/net/can/af_can.c
+++ b/net/can/af_can.c
@@ -451,7 +451,7 @@ 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)))
```