author	Taehee Yoo <ap420073@gmail.com>	2021-07-05 15:38:07 +0000
committer	David S. Miller <davem@davemloft.net>	2021-07-06 10:36:59 -0700
commit	105cd17a866017b45f3c45901b394c711c97bf40 (patch)	
tree	d3fb4428abaa48a8284441a2db9674661054c6c9	
parent	b648eba4c69e5819880b4907e7fcb2bb576069ab (diff)	
download	linux-105cd17a866017b45f3c45901b394c711c97bf40.tar.gz	

diff options

context: 3

space: include

mode: unified

bonding: fix null dereference in bond_ipsec_add_sa()

```
If bond doesn't have real device, bond->curr_active_slave is null.
But bond_ipsec_add_sa() dereferences bond->curr_active_slave without
null checking.
So, null-ptr-deref would occur.

Test commands:
    ip link add bond0 type bond
    ip link set bond0 up
    ip x s add proto esp dst 14.1.1.1 src 15.1.1.1 spi \
0x07 mode transport reqid 0x07 replay-window 32 aead 'rfc4106(gcm(aes))' \
0x44434241343332312423222114131211f4f3f2f1 128 sel src 14.0.0.52/24 \
dst 14.0.0.70/24 proto tcp offload dev bond0 dir in

Splat looks like:
KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007]
CPU: 4 PID: 680 Comm: ip Not tainted 5.13.0-rc3+ #1168
RIP: 0010:bond_ipsec_add_sa+0xc4/0x2e0 [bonding]
Code: 85 21 02 00 00 4d 8b a6 48 0c 00 00 e8 75 58 44 ce 85 c0 0f 85 14
01 00 00 48 b8 00 00 00 00 00 fc ff df 4c 89 e2 48 c1 ea 03 <80> 3c 02
00 0f 85 fc 01 00 00 48 8d bb e0 02 00 00 4d 8b 2c 24 48
RSP: 0018:ffff88810946f508 EFLAGS: 00010246
RAX: dfffc0000000000 RBX: ffff88810b4e8040 RCX: 0000000000000001
RDX: 0000000000000000 RSI: ffffffff8fe34280 RDI: ffff888115abe100
RBP: ffff88810946f528 R08: 0000000000000003 R09: fffffbfff2287e11
R10: 0000000000000001 R11: ffff888115abe0c8 R12: 0000000000000000
R13: ffffffffc0aea9a0 R14: ffff88800d7d2000 R15: ffff88810b4e8330
FS:  00007efc5552e680(0000) GS:ffff888119c00000(0000)
knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 000055c2530dbf40 CR3: 0000000103056004 CR4: 00000000003706e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
Call Trace:
 xfrm_dev_state_add+0x2a9/0x770
 ? memcpy+0x38/0x60
 xfrm_add_sa+0x2278/0x3b10 [xfrm_user]
 ? xfrm_get_policy+0xaa0/0xaa0 [xfrm_user]
 ? register_lock_class+0x1750/0x1750
 xfrm_user_rcv_msg+0x331/0x660 [xfrm_user]
 ? rcu_read_lock_sched_held+0x91/0xc0
 ? xfrm_user_state_lookup.constprop.39+0x320/0x320 [xfrm_user]
 ? find_held_lock+0x3a/0x1c0
 ? mutex_lock_io_nested+0x1210/0x1210
```

```
 ? sched_clock_cpu+0x18/0x170
 netlink_rcv_skb+0x121/0x350
 ? xfrm_user_state_lookup.constprop.39+0x320/0x320 [xfrm_user]
 ? netlink_ack+0x9d0/0x9d0
 ? netlink_deliver_tap+0x17c/0xa50
 xfrm_netlink_rcv+0x68/0x80 [xfrm_user]
 netlink_unicast+0x41c/0x610
 ? netlink_attachskb+0x710/0x710
 netlink_sendmsg+0x6b9/0xb70
[ ...]

Fixes: 18cb261afd7b ("bonding: support hardware encryption offload to slaves")
Signed-off-by: Taehee Yoo <ap420073@gmail.com>
Signed-off-by: David S. Miller <davem@davemloft.net>
```

Diffstat

-rw-r--r-- drivers/net/bonding/bond_main.c 5

1 files changed, 5 insertions, 0 deletions

```
diff --git a/drivers/net/bonding/bond_main.c b/drivers/net/bonding/bond_main.c
index d4d718e04dcc4..5466b24ceab6b 100644
--- a/drivers/net/bonding/bond_main.c
+++ b/drivers/net/bonding/bond_main.c
@@ -411,6 +411,11 @@ static int bond_ipsec_add_sa(struct xfrm_state *xs)
        rcu_read_lock();
        bond = netdev_priv(bond_dev);
        slave = rcu_dereference(bond->curr_active_slave);
+       if (!slave) {
+               rcu_read_unlock();
+               return -ENODEV;
+       }
+
        xs->xso.real_dev = slave->dev;
        bond->xs = xs;
```