general protection fault in bond_ipsec_add_sa (2)

Status: fixed on 2021/11/10 00:50
Reported-by: syzbot+@syzkaller.appspotmail.com
Fix commit: 105cd17a8660 bonding: fix null dereference in bond_ipsec_add_sa()
First crash: 509d, last: 509d

similar bugs (1):

Kernel	Title	Repro	Cause bisect	Fix bisect	Count	Last	Reported	Patched	Status
upstream	general protection fault in bond_ipsec_add_sa				1	713d	709d	0/24	auto-closed as invalid on 2021

Sample crash report:

```
general protection fault, probably for non-canonical address 0xdfffc0000000000: 0000 [#1] PREEMPT SMP KASAN
KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007]
CPU: 1 PID: 9912 Comm: syz-executor.2 Tainted: G        W         5.13.0-syzkaller #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011
RIP: 0010:bond_ipsec_add_sa+0x9e/0x240 drivers/net/bonding/bond_main.c:412
Code: 04 31 ff 89 c3 89 c6 e8 70 25 c1 fc 85 db 0f 85 f6 00 00 00 e8 23 1e c1 fc 4c 89 ea 48 b8 00 00 00 00 00 fc ff df 48
RSP: 0018:ffffc9000271f480 EFLAGS: 00010246
RAX: dfffc0000000000 RBX: 0000000000000000 RCX: ffffc90016f68000
RDX: 0000000000000000 RSI: ffffffff84b4665d RDI: 0000000000000003
RBP: ffff88808a94de00 R08: 0000000000000000 R09: 0000000000000000
R10: ffffffff84b46650 R11: 0000000000000000 R12: ffff8880167b0000
R13: 0000000000000000 R14: ffff88808a94e0d0 R15: ffff88808a94e0e8
FS:  00007f80b964f700(0000) GS:ffff8880b9d00000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 0000000000544038 CR3: 000000006e700000 CR4: 00000000001506e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
Call Trace:
 xfrm_dev_state_add+0x2e2/0x890 net/xfrm/xfrm_device.c:266
 xfrm_state_construct net/xfrm/xfrm_user.c:655 [inline]
 xfrm_add_sa+0x229e/0x35f0 net/xfrm/xfrm_user.c:684
 xfrm_user_rcv_msg+0x42c/0x8b0 net/xfrm/xfrm_user.c:2812
 netlink_rcv_skb+0x153/0x420 net/netlink/af_netlink.c:2504
 xfrm_netlink_rcv+0x6b/0x90 net/xfrm/xfrm_user.c:2824
```

Crashes (1):

Manager	Time	Kernel	Commit	Syzkaller	Config	Log	Report	Syz repro	C repro	VM info	
ci-upstream-net-kasan-gce	2021/07/05 17:53	net-next	5e437416ff66	55aa55c2	.config	log	report			info	general protection f

* ~~Struck through~~ repros no longer work on HEAD.