nfc: fix NULL ptr dereference in llcp_sock_getname() after failed con…

Browse files

```
…nect

It's possible to trigger NULL pointer dereference by local unprivileged
user, when calling getsockname() after failed bind() (e.g. the bind
fails because LLCP_SAP_MAX used as SAP):

  BUG: kernel NULL pointer dereference, address: 0000000000000000
  CPU: 1 PID: 426 Comm: llcp_sock_getna Not tainted 5.13.0-rc2-next-20210521+ #9
  Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.14.0-1 04/01/2014
  Call Trace:
   llcp_sock_getname+0xb1/0xe0
   __sys_getpeername+0x95/0xc0
   ? lockdep_hardirqs_on_prepare+0xd5/0x180
   ? syscall_enter_from_user_mode+0x1c/0x40
   __x64_sys_getpeername+0x11/0x20
   do_syscall_64+0x36/0x70
   entry_SYSCALL_64_after_hwframe+0x44/0xae

This can be reproduced with Syzkaller C repro (bind followed by
getpeername):
https://syzkaller.appspot.com/x/repro.c?x=14def446e00000

Cc: <stable@vger.kernel.org>
Fixes: d646960 ("NFC: Initial LLCP support")
Reported-by: syzbot+80fb126e7f7d8b1a5914@syzkaller.appspotmail.com
Reported-by: butt3rflyh4ck <butterflyhuangxx@gmail.com>
Signed-off-by: Krzysztof Kozlowski <krzysztof.kozlowski@canonical.com>
Link: https://lore.kernel.org/r/20210531072138.5219-1-krzysztof.kozlowski@canonical.com
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
```

master

v6.1 … v5.13-rc5

krzk authored and kuba-moo committed on Jun 1, 20211 parent 593f555 commit 4ac06a1e013cf5fdd963317ffd3b968560f33bba

Showing **1 changed file** with **2 additions** and **0 deletions**.

Split Unified

2 net/nfc/llcp_sock.c

```diff
 	if (!llcp_sock->service_name) {
 		nfc_llcp_local_put(llcp_sock->local);
 		llcp_sock->local = NULL;
+		llcp_sock->dev = NULL;
 		ret = -ENOMEM;
 		goto put_dev;
 	}
 		llcp_sock->local = NULL;
 		kfree(llcp_sock->service_name);
 		llcp_sock->service_name = NULL;
+		llcp_sock->dev = NULL;
 		ret = -EADDRINUSE;
 		goto put_dev;
 	}
```

0 comments on commit 4ac06a1

Please sign in to comment.