OsmoPCU - Bug #4725

osmo-pcu segfaults if the BSSGP handler fails to bind()

08/20/2020 05:37 PM - fixeria

Status:	Rejected	**Start date:**	08/21/2020
Priority:	Normal	**Due date:**	
Assignee:	fixeria	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

How to reproduce?

Run any test case from ttcn3-pcu-test with the following NS configuration (see PCU_Tests.cfg):

```
SGSN_Components.mp_nsconfig := {
        local_ip := "127.0.0.1",
        local_udp_port := 80, // <--- (!)
        remote_ip := "127.0.0.1",
        remote_udp_port := 22000,
        nsvci := 1234,
        nsei := 1234
};
```

against osmo-pcu running as a normal (non-root) user.

NOTE: make sure that https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/19744 is applied, otherwise we send remote port as local, and vice versa.

What happens?

```
Program received signal SIGSEGV (fault address 0x100108)
pwndbg> bt
#0  llist_del (entry=0x5555556732a0) at ../../include/osmocom/core/linuxlist.h:129
#1  gprs_nsvc_delete (nsvc=0x5555556732a0) at gprs_ns.c:357
#2  0x00007ffff7f78e45 in gprs_ns_close (nsi=0x555555672d30) at gprs_ns.c:1928
#3  0x00007ffff7f78ea9 in gprs_ns_destroy (nsi=0x555555672d30) at gprs_ns.c:1950
#4  0x0000555555555714f2 in gprs_bssgp_destroy() ()
#5  0x0000555555579191 in pcu_rx_info_ind(gsm_pcu_if_info_ind*) ()
#6  0x000055555557aa3a in pcu_rx(unsigned char, gsm_pcu_if*) ()
#7  0x000055555559d0ea in pcu_sock_read(osmo_fd*) ()
#8  0x000055555559d2cc in pcu_sock_cb(osmo_fd*, unsigned int) ()
#9  0x00007ffff7ce362b in osmo_fd_disp_fds (_eset=<optimized out>, _wset=<optimized out>, _rset=<o
ptimized out>) at select.c:227
#10 _osmo_select_main (polling=<optimized out>) at select.c:265
#11 0x00007ffff7ce3c67 in osmo_select_main (polling=<optimized out>) at select.c:274
#12 0x000055555556e4c6 in main ()
#13 0x00007ffff77ba002 in __libc_start_main () from /usr/lib/libc.so.6
#14 0x000055555556da3e in _start ()
```

It looks like gprs_ns_close() is called twice, and thus gprs_nsvc_delete() too. The later calls llist_del(), so first time nsvc->list gets poisoned (see LLIST_POISON1 and LLIST_POISON2), and second time we crash:

```
pwndbg> p ((struct gprs_ns_inst *) 0x555555672d30)->unknown_nsvc->list
$1 = {
  next = 0x100100, // LLIST_POISON1
  prev = 0x200200  // LLIST_POISON2
}
```

History

#1 - 11/25/2020 06:34 PM - pespin

fixeria wasn't this reproduced with a TTCN3 and already fixed?

#2 - 11/30/2020 01:09 PM - fixeria

- Status changed from New to Feedback

- Assignee set to fixeria

> fixeria wasn't this reproduced with a TTCN3 and already fixed?

I don't think it was fixed nor reproduced. Let me re-try with the recent version.

#3 - 11/30/2020 01:15 PM - fixeria

- Status changed from Feedback to Rejected

Looks like it has been fixed meanwhile, not a problem anymore:

```
DLGLOBAL ERROR socket.c:550 unable to bind socket: 0.0.0.0:80: Permission denied
DBSSGP ERROR gprs_bssgp_pcu.cpp:967 Failed to bind to 0.0.0.0:80
DBSSGP ERROR gprs_bssgp_pcu.cpp:976 Failed to bind to any NS-VC
DBSSGP ERROR gprs_bssgp_pcu.cpp:1103 Failed to connect!
DL1IF ERROR pcu_l1_if.cpp:682 No NSVC available to connect to the SGSN!
```