OsmoPCU - Bug #4029

osmo-pcu: several runtime errors detected by ASan

05/27/2019 05:29 PM - pespin

Status: Resolved
Priority: Normal
Assignee: pespin
% Done: 100%

Description

Seen today while operating my network locally (master as of date of today, osmo-pcu eb64d43922f48901ea4f872b5c2d65b9e334221)

osmo-pcu/src/tbf_ul.cpp:392 LLC [PCU -> SGSN] TBF(TFI=0 TLLI=0xd6f1f98f DIR=UL STATE=FLOW) len=16 include/osmocom/core/msgb.h:543:2: runtime error: variable length array bound evaluates to non-positive value -1

And another different one:

20190527190229251 DTBFUL <000a> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp:295 TBF(TFI=0 TLLI=0xd6f1f98f DIR=UL STATE=FLOW) len=16 include/osmocom/core/msgb.h:543:2: runtime error: variable length array bound evaluates to non-positive value -1

Associated revisions

03/09/2022 1/4
msgb: Allow size==headroom in msgb_alloc_headroom() 

Nothing really forbids this case, it's totally fine allocating all space of msgb as headroom. osmo-pcu actually does that in gprs_rlc_mac_ul_tbf:_snd_ul_ud().

Related: OS#4029
Change-Id: Ibe05d08e3169a2603e891f76682a3b352a93ec7a

History
#1 - 07/23/2019 01:50 PM - pespin
- Assignee set to sysmocom

Seen again while starting PCU together with the whole 2G network:

```
20190723154714063 DL1IF <0001> /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_l1_if.cpp:125 Sending activate request: trx=0 ts=6
20190723154714063 DL1IF <0001> /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_l1_if.cpp:569 PDCH: trx=0 ts=6
20190723154714063 DL1IF <0001> /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_l1_if.cpp:125 Sending activate request: trx=0 ts=7
20190723154714063 DNS <000b> /home/pespin/dev/sysmocom/git/libosmocore/src/gb/gprs_ns.c:1355 NSVCI=1800 Rx NS RESET ACK (NSEI=1800, NSVCI=1800)
20190723154714063 DNS <000b> /home/pespin/dev/sysmocom/git/libosmocore/src/gb/gprs_ns.c:704 NSEI=1800 Tx NS UNBLOCK (NSVCI=1800)
20190723154714064 DNS <000b> /home/pespin/dev/sysmocom/git/libosmocore/src/gb/gprs_ns.c:1805 NSEI=1800 Rx NS UNBLOCK ACK
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:537 NS-VC 1800 is unblocked.
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:616 Sending reset on BVCI 0
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:282 RxBSSGP BVCI=0
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/libosmocore/src/gb/gprs_bssgp_bss.c:280 BSSGP (BVCI=1800) Tx BVC-UNBLOCK
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/libosmocore/src/gb/gprs_bssgp_bss.c:293 RxBSSGP BVCI=1800
20190723154714064 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:1071 Allocating DL TBF: MS_CLASS=0/0
20190723154714064 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:979 Allocating UL TBF: MS_CLASS=0/0
20190723154714064 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:540 TBF(TFI=0 TLLI=0x00000000 DIR=UL STATE=NULL) Setting Control TS 6
20190723154714064 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:762 TBF(TFI=0 TLLI=0x00000000 DIR=UL STATE=FLOW) set ass. type CCCH [prev CCCH:0, PACCH:0]
03/09/2022
```
This actually usbns, exporting UBSAN_OPTIONS=print_stacktrace=1:halt_on_error=1 should help.

Should be fixed by https://gerrit.osmocom.org/c/libosmocore/+/15607 msgb: Allow size==headroom in msgb_alloc_headroom(*)

Once merged the ticket can be closed.

The other runtime issue was already fixed by Hoernchen in osmo-pcu.git abbb01effdece38a19385e6a58e3b719a57710b2

Assignee changed from sysmocom to pespin
#7 - 10/03/2019 02:46 PM - pespin

- Status changed from Feedback to Resolved
- % Done changed from 90 to 100

Merged, closing.