OsmoPCU - Bug #4029

osmo-pcu: several runtime errors detected by ASan

05/27/2019 05:29 PM - pespin

Status: Resolved
Priority: Normal
Assignee: pespin
Due date: 05/27/2019
% Done: 100%

Description

Seen today while operating my network locally (master as of date of today, osmo-pcu eb64d43922f48901ea4fc87b5c2d65b9e334221)

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

History

05/15/2020
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 DL1IF <0001> /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_l1_if.cpp:569 PDCH: 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 Rx NS UN BLOCK (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_bss.cpp:282 Sending unlock on BVCI 1800
```

This actually ubsan, exporting UBSAN_OPTIONS=print_stacktrace=1:halt_on_error=1 should help.

#2 - 07/23/2019 02:57 PM - Hoernchen

#3 - 07/23/2019 04:57 PM - pespin
20190723185650062 DL1IF <0001> /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_l1_if.cpp:390 RACH request received: sapi=1 gta=0, ra=123, fn=750984, cur_fn=750984, is_11bit=0  
20190723185650063 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  
20190723185650063 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:925 TBF(TFI=0 TLLI=0x00000000 DIR=UL STATE=FLOW) Allocated: trx = 0, ul_slots = 40, dl_slots = 00  
20190723185650063 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:770 TBF(TFI=0 TLLI=0x00000000 DIR=UL STATE=FLOW) TX: START Immediate Assignment Uplink (AGCH)  
20190723185650063 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/bts.cpp:762 TBF(TFI=0 TLLI=0x00000000 DIR=UL STATE=FLOW) set ass. type CCCH [prev CCCH:0, PACCH:0]  
20190723185650063 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/bts.cpp:770 TBF(TFI=0 TLLI=0x00000000 DIR=UL STATE=FLOW) TX: START Immediate Assignment Uplink (AGCH)  
20190723185650063 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:295 TBF(TFI=0 TLLI=0x00000000 DIR=UL STATE=FLOW) Decoded premier TLLI=0x00000000 of UL DATA TFI=0.  
#0 0x559e4a7f7f2ed in msgb_alloc_headroom /home/pespin/dev/sysmocom/build/new/out/include/osmocom/core/msgb.h:543:2: runtime error: variable length array bound evaluates to non-positive value -1  
#1 0x559e4a785a3b in gprs_lcmac_ul_tbf::snd_ul_ud() /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp:399  
#2 0x559e4a78042a in gprs_lcmac_ul_tbf::assemble_forward_llc(gprs_rlc_data const*) /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp:98  
#3 0x559e4a784637 in gprs_lcmac_ul_tbf::rcv_data_block_authorized(gprs_rlc_data_info const*, unsigned char*, pcu_l1_meas*) /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp:318  
#4 0x559e4a7b3b3b in gprs_lcmac_pdch::rcv_data_block(unsigned char*, unsigned char, unsigned int, pcu_l1_meas*, GprsCodingScheme) /home/pespin/dev/sysmocom/git/osmo-pcu/src/pdch.cpp:812  
#5 0x559e4a7b401c in gprs_lcmac_pdch::rcv_block_gprs(unsigned char*, unsigned char, unsigned int, pcu_l1_meas*, GprsCodingScheme) /home/pespin/dev/sysmocom/git/osmo-pcu/src/pdch.cpp:825  
#6 0x559e4a7b3129 in gprs_lcmac_pdch::rcv_block(unsigned char*, unsigned char, unsigned int, pcu_l1_meas*) /home/pespin/dev/sysmocom/git/osmo-pcu/src/pdch.cpp:745  
#7 0x559e4a748781 in pcu_rx_data_ind_pdch /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_l1_if.cpp:253  
#8 0x559e4a74892f in pcu_rx_data_ind /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_l1_if.cpp:300  
#9 0x559e4a751583 in pcu_rx(unsigned char, gsm_pcu_if*) /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_l1_if.cpp:629  
#10 0x559e4a7e060f in pcu_sock_read /home/pespin/dev/sysmocom/git/osmo-pcu/src/osmosbs_sock.cpp:162  
#11 0x559e4a7e0ce3 in pcu_sock_cl /home/pespin/dev/sysmocom/git/osmo-pcu/src/osmosbs_sock.cpp:229  
#12 0x7f59a9a37b83 0x7f59a9a37b83 in osmo_fd_disp_fds /home/pespin/dev/sysmocom/git/libosmocore/src/select.c:223  
#13 0x7f59a9a37b83 in osmo_select_main /home/pespin/dev/sysmocom/git/libosmocore/src/select.c:223  
#14 0x559e4a71a369 in main /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_main.cpp:361  
#15 0x7f59a9a79760 in __libc_start_main (/usr/lib/libc.so.6+0x23ce2)  
#16 0x559e4a716c7d in __start (/home/pespin/dev/sysmocom/build/new/out/bin/osmo-pcu+0x1efc7d)  

#4 - 09/26/2019 03:53 PM - pespin  
- Status changed from New to Feedback  
- % Done changed from 0 to 90  

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.  

#5 - 09/26/2019 04:07 PM - pespin  

The other runtime issue was already fixed by @Hoernchen in osmo-pcu.git abbb01efdc38a19385e6a58e3b719a57710b02  

#6 - 09/26/2019 04:08 PM - pespin  
- 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.