OsmoPCU - Bug #4029

osmo-pcu: several runtime errors detected by ASan

05/27/2019 05:29 PM - pespin

Status:	Resolved	**Start date:**	05/27/2019
Priority:	Normal	**Due date:**	
Assignee:	pespin	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

Seen today while operating my network locally (master as of date of today, osmo-pcu eb64d43922f48901ea4fc872b5c2d65b9e334221)

```
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-pos
itive 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=0x00000000 DIR=UL STATE=FLOW) Decoded premier TLLI=0x00000000 of UL DATA TFI=0.
20190527190229251 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp:392 LLC [PCU
 -> SGSN] TBF(TFI=0 TLLI=0xcf38987f DIR=UL STATE=FLOW) len=10
20190527190229252 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:189
LLC [SGSN -> PCU] = TLLI: 0xcf38987f IMSI: 901700000015254 len: 8
20190527190229252 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:1071 Allocating D
L TBF: MS_CLASS=0/0
20190527190229252 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:540 TBF(TFI=0 TLL
I=0x00000000 DIR=DL STATE=NULL) Setting Control TS 6
20190527190229252 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:925 TBF(TFI=0 TLL
I=0xcf38987f DIR=DL STATE=NULL) Allocated: trx = 0, ul_slots = 40, dl_slots = 40
20190527190229252 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/bts.cpp:814 TBF(TFI=0 TLL
I=0xcf38987f DIR=DL STATE=ASSIGN) TX: START Immediate Assignment Downlink (PCH)
20190527190229270 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_ms.cpp:645 Un
able to update UL (M)CS CS-2 because we don't have link quality measurements.
20190527190229293 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_ms.cpp:645 Un
able to update UL (M)CS CS-2 because we don't have link quality measurements.
20190527190229311 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_ms.cpp:645 Un
able to update UL (M)CS CS-2 because we don't have link quality measurements.
20190527190229328 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_ms.cpp:645 Un
able to update UL (M)CS CS-2 because we don't have link quality measurements.
20190527190229352 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_ms.cpp:645 Un
able to update UL (M)CS CS-2 because we don't have link quality measurements.
20190527190229371 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_ms.cpp:645 Un
able to update UL (M)CS CS-2 because we don't have link quality measurements.
20190527190229390 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_ms.cpp:645 Un
able to update UL (M)CS CS-2 because we don't have link quality measurements.
20190527190229413 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_ms.cpp:645 Un
able to update UL (M)CS CS-2 because we don't have link quality measurements.
20190527190229430 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_ms.cpp:645 Un
able to update UL (M)CS CS-2 because we don't have link quality measurements.
20190527190229490 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_rlcmac_meas.c
pp:106 UL RSSI of TLLI=0xcf38987f: -35 dBm
20190527190229490 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:484 TBF(TFI=0 TLL
I=0xcf38987f DIR=UL STATE=FINISHED) free
/home/pespin/dev/sysmocom/git/osmo-pcu/src/bts.cpp:554:19: runtime error: left shift of 220 by 28
places cannot be represented in type 'int'
```

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 r
equest: 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 r
equest: 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 Tx NS UN
BLOCK (NSVCI=1800)
20190723154714064 DNS <000b> /home/pespin/dev/sysmocom/git/libosmocore/src/gb/gprs_ns.c:1805 NSEI=1800 Rx NS U
NBLOCK ACK
20190723154714064 DPCU <000d> /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:816 Sending rese
t on BVCI 0
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/libosmocore/src/gb/gprs_bssgp_bss.c:300 BSSGP (B
VCI=0) Tx BVC-RESET CAUSE=O&M intervention
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:282 Rx BSSGP BVC
I=-1 (SIGN) BVC_RESET_ACK
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:824 Sending rese
t on BVCI 1800
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/libosmocore/src/gb/gprs_bssgp_bss.c:300 BSSGP (B
VCI=1800) Tx BVC-RESET CAUSE=O&M intervention
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:282 Rx BSSGP BVC
I=-1 (SIGN) BVC_RESET_ACK
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:832 Sending unbl
ock on BVCI 1800
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/libosmocore/src/gb/gprs_bssgp_bss.c:280 BSSGP (B
VCI=1800) Tx BVC-UNBLOCK
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:293 Rx BSSGP BVC
I=-1 (SIGN) BVC_UNBLOCK_ACK
20190723154715034 DL1IF <0001> /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_l1_if.cpp:390 RACH request recei
ved: sapi=1 qta=0, ra=120, fn=2270537, cur_fn=2270541, is_11bit=0
20190723154715034 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:979 Allocating UL TBF: MS_CLA
SS=0/0
20190723154715034 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
20190723154715034 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:925 TBF(TFI=0 TLLI=0x00000000
 DIR=UL STATE=NULL) Allocated: trx = 0, ul_slots = 40, dl_slots = 00
20190723154715034 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]
20190723154715034 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)
20190723154715287 DTBFUL <000a> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp:295 TBF(TFI=0 TLLI=0x000
00000 DIR=UL STATE=FLOW) Decoded premier TLLI=0x00000000 of UL DATA TFI=0.
20190723154715310 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp:392 LLC [PCU -> SGSN] TB
F(TFI=0 TLLI=0xd01d83b2 DIR=UL STATE=FLOW) len=51
/home/pespin/dev/sysmocom/build/new/out/include/osmocom/core/msgb.h:543:2: runtime error: variable length arra
y bound evaluates to non-positive value -1        <--------------------
20190723154715311 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:160 LLC [SGSN ->
 PCU] = TLLI: 0xd01d83b2 IMSI:  len: 12
20190723154715311 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:1071 Allocating DL TBF: MS_CL
ASS=0/0
20190723154715311 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:540 TBF(TFI=0 TLLI=0x00000000
 DIR=DL STATE=NULL) Setting Control TS 6
20190723154715311 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:925 TBF(TFI=0 TLLI=0xd01d83b2
 DIR=DL STATE=NULL) Allocated: trx = 0, ul_slots = 40, dl_slots = c0
```

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

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

#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 recei
ved: sapi=1 qta=0, ra=123, fn=750980, cur_fn=750984, is_11bit=0
20190723185650062 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:979 Allocating UL TBF: MS_CLA
SS=0/0
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=NULL) Allocated: trx = 0, ul_slots = 40, dl_slots = 00
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)
20190723185650375 DTBFUL <000a> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp:295 TBF(TFI=0 TLLI=0x000
00000 DIR=UL STATE=FLOW) Decoded premier TLLI=0x00000000 of UL DATA TFI=0.
20190723185650417 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp:392 LLC [PCU -> SGSN] TB
F(TFI=0 TLLI=0x7f4d37b5 DIR=UL STATE=FLOW) len=54
/home/pespin/dev/sysmocom/build/new/out/include/osmocom/core/msgb.h:543:2: runtime error: variable length arra
y bound evaluates to non-positive value -1
    #0 0x559e4a77f2ed in msgb_alloc_headroom /home/pespin/dev/sysmocom/build/new/out/include/osmocom/core/msgb
.h:543
    #1 0x559e4a785a3b in gprs_rlcmac_ul_tbf::snd_ul_ud() /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp
:399
    #2 0x559e4a78042a in gprs_rlcmac_ul_tbf::assemble_forward_llc(gprs_rlc_data const*) /home/pespin/dev/sysmo
com/git/osmo-pcu/src/tbf_ul.cpp:98
    #3 0x559e4a784637 in gprs_rlcmac_ul_tbf::rcv_data_block_acknowledged(gprs_rlc_data_info const*, unsigned c
har*, pcu_l1_meas*) /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf_ul.cpp:318
    #4 0x559e4a7b3db3 in gprs_rlcmac_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_rlcmac_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_rlcmac_pdch::rcv_block(unsigned char*, unsigned char, unsigned int, pcu_l1_meas*
) /home/pespin/dev/sysmocom/git/osmo-pcu/src/pdch.cpp:745
    #7 0x559e4a747871 in pcu_rx_data_ind_pdtch /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/osmobts_sock.cpp:162
    #11 0x559e4a7e0ce3 in pcu_sock_cb /home/pespin/dev/sysmocom/git/osmo-pcu/src/osmobts_sock.cpp:229
    #12 0x7f59a98a7893 in osmo_fd_disp_fds /home/pespin/dev/sysmocom/git/libosmocore/src/select.c:223
    #13 0x7f59a98a7bb9 in osmo_select_main /home/pespin/dev/sysmocom/git/libosmocore/src/select.c:263
    #14 0x559e4a71a369 in main /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_main.cpp:361
    #15 0x7f59a87c7ce2 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 ab8b01effdce38a19385e6a58e3b719a57710b02

#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.