**OsmoPCU - Bug #4029**

**osmo-pcu: several runtime errors detected by ASan**

05/27/2019 05:29 PM - pespin

<table>
<thead>
<tr>
<th>Status</th>
<th>Resolved</th>
<th>Priority</th>
<th>Normal</th>
<th>Assignee</th>
<th>pespin</th>
<th>Start date</th>
<th>05/27/2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Due date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% Done</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100%</td>
</tr>
</tbody>
</table>

**Category:**

**Description**

Seen today while operating my network locally (master as of date of today, osmo-pcu eb64d43922f48901ea4fc8725c2d65b9e334221)

```
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=0xfd0198f 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

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 DL TBF: MS_CLASS=0/0
20190527190229252 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
20190527190229252 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/tbf.cpp:925 TBF(TFI=0 TLLI=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 Unable 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 Unable 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 Unable 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 Unable to update UL (M)CS CS-2 because we don't have link quality measurements.
20190527190229335 DRLCMACMEAS <0007> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_ms.cpp:645 Unable 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 Unable 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 Unable 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 Unable 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 Unable 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_tacac_meas.cpp: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 TLLI=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'
```

**Associated revisions**

08/08/2021
Revision ec4b6270 - 09/26/2019 03:46 PM - pespin

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_rlcmac_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/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 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:816 Sending reset on BVCI 0
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:302 BSSGP (BVCI=0) Tx BVC-RESET CAUSE=O&M intervention
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:824 Sending reset on BVCI 1800
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:282 BSSGP (BVCI=1800) Tx BVC-UNBLOCK
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:293 Rx BSSGP BVCI UNBLOCK ACK
20190723154714064 DBSSGP <000c> /home/pespin/dev/sysmocom/git/osmo-pcu/src/gprs_bssgp_pcu.cpp:282 BSSGP (BVCI=1800) Tx BVC-UNBLOCK ACK
20190723154715034 DL1IF <0001> /home/pespin/dev/sysmocom/git/osmo-pcu/src/pcu_l1_if.cpp:390 RACH request received: 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_CLASS=0/0
20190723154715034 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/bts.cpp:753 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) Decoded premier TLLI=0x00000000 of UL DATA TFI=0.
20190723154715034 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/bts.cpp:822 Allocating UL TBF: MS_CLASS=0/0
20190723154715034 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/bts.cpp:824 BSSGP (BVCI=0) Tx BVC-UNBLOCK ACK
20190723154715034 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/bts.cpp:832 Sending unblock on BVCI 1800
20190723154715034 DTBF <0008> /home/pespin/dev/sysmocom/git/osmo-pcu/src/bts.cpp:280 BSSGP (BVCI=1800) Tx BVC-UNBLOCK

08/08/2021
#2 - 07/23/2019 02:57 PM - Hoernchen

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

#3 - 07/23/2019 04:57 PM - pespin

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

#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 ab8b01eefdce38a193856e6a58e3b719a57710b02

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

- Assignee changed from sysmocom to pespin
Merged, closing.