OsmoPCU - Bug #5206

Crash: SEGV on current master 945be910 around gprs_rlcmac_tbf::name

08/06/2021 04:40 PM - iedemam

Status:	Feedback	**Start date:**	08/06/2021
Priority:	High	**Due date:**	
Assignee:	iedemam	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

Log Tail

```
<0008> tbf.cpp:629 TBF(TFI=10 TLLI=0x78f93c4f DIR=UL STATE=ASSIGN EGPRS) poll timeout for FN=16133
91, TS=7 (curr FN 1613395)
<0002> bts.cpp:303 Detected FN jump! 1613395 -> 1613404
<0002> bts.cpp:303 Detected FN jump! 1613404 -> 1613412
<0002> pdch.cpp:318 PDCH(bts=0,trx=1,ts=7) PACKET CONTROL ACK with unknown FN=1613412 TLLI=0x8a422
e00 (TRX 1 TS 7)
<0002> pdch.cpp:328 PDCH(bts=0,trx=1,ts=7) PACKET CONTROL ACK with unknown TBF corresponds to MS w
ith IMSI 000, TA 0, uTBF (TFI=0, state=None), dTBF (TFI=5, state=FLOW)
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=7) Expiring FN=1613412 but previous FN=1613404
 is still reserved!
<0002> pdch_ul_controller.c:329 PDCH(bts=0,trx=1,ts=7) Timeout for registered POLL (FN=1613404): T
BF(TFI=5 TLLI=0x7a771851 DIR=UL STATE=RELEASING EGPRS)
<0008> tbf.cpp:629 TBF(TFI=5 TLLI=0x7a771851 DIR=UL STATE=RELEASING EGPRS) poll timeout for FN=161
3404, TS=7 (curr FN 1613412)
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=7) Expiring FN=1613412 but previous FN=1613408
 is still reserved!
<0002> pdch_ul_controller.c:329 PDCH(bts=0,trx=1,ts=7) Timeout for registered POLL (FN=1613408): T
BF(TFI=1 TLLI=0x7b29abc1 DIR=UL STATE=RELEASING EGPRS)
<0008> tbf.cpp:629 TBF(TFI=1 TLLI=0x7b29abc1 DIR=UL STATE=RELEASING EGPRS) poll timeout for FN=161
3408, TS=7 (curr FN 1613412)
<0008> pdch.cpp:350 TBF(TFI=12 TLLI=0x8b021f0e DIR=UL STATE=FINISHED EGPRS) Recovered uplink ack f
or UL
<0008> ./tbf.h:376 TBF(DL-TFI_12)[7e86c0]{ASSIGN}: transition to state ASSIGN not permitted!
<0002> bts.cpp:303 Detected FN jump! 1613417 -> 1613425
<0008> tbf.cpp:458 TBF(TFI=1 TLLI=0x7b29abc1 DIR=UL STATE=RELEASING EGPRS) T3195 timeout expired,
freeing TBF
<0008> tbf.cpp:462 TBF(TFI=1 TLLI=0x7b29abc1 DIR=UL STATE=RELEASING EGPRS) T3195 timeout expired,
freeing TBF: |Assignment was on PACCH|Uplink data was received|
<0008> pdch.cpp:405 TBF(TFI=9 TLLI=0x9ac07500 DIR=UL STATE=FLOW EGPRS) Recovered uplink assignment
 for UL
<0002> bts.cpp:303 Detected FN jump! 1613430 -> 1613438
<0008> tbf.cpp:458 TBF(TFI=3 TLLI=0x7ba82931 DIR=UL STATE=RELEASING EGPRS) T3195 timeout expired,
freeing TBF
<0008> tbf.cpp:462 TBF(TFI=3 TLLI=0x7ba82931 DIR=UL STATE=RELEASING EGPRS) T3195 timeout expired,
freeing TBF: |Assignment was on PACCH|Uplink data was received|
<0008> tbf.cpp:793 TBF(TFI=10 TLLI=0x7b29abc1 DIR=DL STATE=ASSIGN EGPRS) releasing due to PACCH as
signment timeout.
<0002> bts.cpp:303 Detected FN jump! 1613438 -> 1613451
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=7) Expiring FN=1613456 but previous FN=1613434
 is still reserved!
<0002> pdch_ul_controller.c:329 PDCH(bts=0,trx=1,ts=7) Timeout for registered POLL (FN=1613434): T
BF(TFI=11 TLLI=0x7c32b6f0 DIR=UL STATE=ASSIGN EGPRS)
<0008> tbf.cpp:629 TBF(TFI=11 TLLI=0x7c32b6f0 DIR=UL STATE=ASSIGN EGPRS) poll timeout for FN=16134
34, TS=7 (curr FN 1613456)
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=7) Expiring FN=1613456 but previous FN=1613438
 is still reserved!
<0002> pdch_ul_controller.c:329 PDCH(bts=0,trx=1,ts=7) Timeout for registered POLL (FN=1613438): T
BF(TFI=10 TLLI=0x78f93c4f DIR=UL STATE=ASSIGN EGPRS)
```

```
<0008> tbf.cpp:629 TBF(TFI=10 TLLI=0x78f93c4f DIR=UL STATE=ASSIGN EGPRS) poll timeout for FN=16134
38, TS=7 (curr FN 1613456)
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=7) Expiring FN=1613456 but previous FN=1613443
 is still reserved!
<0002> pdch_ul_controller.c:329 PDCH(bts=0,trx=1,ts=7) Timeout for registered POLL (FN=1613443): T
BF(TFI=5 TLLI=0x7a771851 DIR=UL STATE=RELEASING EGPRS)
<0008> tbf.cpp:629 TBF(TFI=5 TLLI=0x7a771851 DIR=UL STATE=RELEASING EGPRS) poll timeout for FN=161
3443, TS=7 (curr FN 1613456)
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=7) Expiring FN=1613456 but previous FN=1613447
 is still reserved!
```

Backtrace

```
Program received signal SIGSEGV, Segmentation fault.
gprs_rlcmac_tbf::name (this=0x7ffff7fa3060) at tbf.cpp:1070
1070    tbf.cpp: No such file or directory.
#0  gprs_rlcmac_tbf::name (this=0x7ffff7fa3060) at tbf.cpp:1070
#1  0x000000000041905a in tbf_name (tbf=<optimized out>) at tbf.cpp:1065
#2  0x000000000042ad01 in pdch_ulc_expire_fn (ulc=0x7bd690, fn=fn@entry=1613456) at pdch_ul_contro
ller.c:327
#3  0x000000000040ff0b in pcu_rx_data_ind_pdtch (bts=bts@entry=0x7ad200, pdch=pdch@entry=0x7af720,
 data=data@entry=0x7fffffffe326 "@\006I0\235\033", '+' <repeats 17 times>, len=<optimized out>, fn
=1613456, meas=meas@entry=0x7fffffffe2a0) at pcu_l1_if.cpp:285
#4  0x0000000000410834 in pcu_rx_data_ind (data_ind=0x7fffffffe324, bts=0x7ad200) at pcu_l1_if.cpp
:418
#5  pcu_rx (pcu_prim=pcu_prim@entry=0x7fffffffe320, pcu_prim_length=<optimized out>) at pcu_l1_if.
cpp:992
#6  0x0000000000431399 in pcu_sock_read (bfd=<optimized out>) at osmobts_sock.c:156
#7  0x0000000000431585 in pcu_sock_cb (bfd=0x6974e0 <pcu_sock_state>, flags=1) at osmobts_sock.c:2
11
#8  0x00007ffff6c8e78c in ?? () from /usr/lib64/libosmocore.so.17
#9  0x00007ffff6c8e836 in osmo_select_main () from /usr/lib64/libosmocore.so.17
#10 0x0000000000406bf5 in main (argc=1, argv=0x7fffffffecd8) at pcu_main.cpp:329
$1 = {si_signo = 11, si_errno = 0, si_code = 1, _sifields = {_pad = {-134469780, 32767, 160, 0, 76
272, 0, 41715216, 0, 1885845516, 32767, -525481846, 32588, 1, 0, 160, 0, 29765600, 0, 40527024, 0,
 44, 0, 6622689, 0, 8149536, 0, 38710912, 0}, _kill = {si_pid = -134469780, si_uid = 32767}, _time
r = {si_tid = -134469780, si_overrun = 32767, si_sigval = {sival_int = 160, sival_ptr = 0xa0}}, _r
t = {si_pid = -134469780, si_uid = 32767, si_sigval = {sival_int = 160, sival_ptr = 0xa0}}, _sigch
ld = {si_pid = -134469780, si_uid = 32767, si_status = 160, si_utime = 327585745600512, si_stime =
 179165488465575936}, _sigfault = {si_addr = 0x7ffff7fc276c, _addr_lsb = 160, _addr_bnd = {_lower
= 0x129f0, _upper = 0x27c8610}}, _sigpoll = {si_band = 140737353885548, si_fd = 160}}}
```

History

#1 - 08/06/2021 04:48 PM - iedemam

I've seen this now with a different call stack but it looks like the same kaboom.

Log Tail Type 2

```
<0002> gprs_rlcmac_ts_alloc.cpp:776 No USF available
<0008> tbf.cpp:746 TBF(TFI=0 TLLI=0x78474a51 DIR=UL STATE=NULL EGPRS) Timeslot Allocation failed: trx = 1, sin
gle_slot = 0
<0008> tbf_ul.cpp:151 MS(TLLI=0x78474a51, IMSI=618010111567897, TA=0, 12/12, DL) No PDCH resource
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=6) Expiring FN=1792717 but previous FN=1792708 is still re
served!
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=6) Expiring FN=1792717 but previous FN=1792713 is still re
served!
<0002> pdch_ul_controller.c:329 PDCH(bts=0,trx=1,ts=6) Timeout for registered POLL (FN=1792713): TBF(TFI=3 TLL
I=0xe2569340 DIR=DL STATE=FLOW EGPRS)
<0008> tbf.cpp:629 TBF(TFI=3 TLLI=0xe2569340 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1792713, TS=6 (curr
FN 1792717)
<0008> tbf.cpp:699 TBF(TFI=3 TLLI=0xe2569340 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK:
 |Assignment was on PACCH|Downlink ACK was received|
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=6) Expiring FN=1792734 but previous FN=1792721 is still re
served!
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=6) Expiring FN=1792734 but previous FN=1792726 is still re
served!
```

```
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=6) Expiring FN=1792734 but previous FN=1792730 is still re
served!
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=7) Expiring FN=1792734 but previous FN=1792730 is still re
served!
<0008> tbf.cpp:458 TBF(TFI=7 TLLI=0xcb2f0a00 DIR=DL STATE=WAIT_RELEASE EGPRS) T3193 timeout expired, freeing T
BF
<0008> tbf.cpp:465 TBF(TFI=7 TLLI=0xcb2f0a00 DIR=DL STATE=WAIT_RELEASE EGPRS) T3193 timeout expired, freeing T
BF
<0008> tbf.cpp:458 TBF(TFI=14 TLLI=0xee10ac00 DIR=DL STATE=WAIT_RELEASE EGPRS T3193 timeout expired, freeing T
BF
<0008> tbf.cpp:465 TBF(TFI=14 TLLI=0xee10ac00 DIR=DL STATE=WAIT_RELEASE EGPRS T3193 timeout expired, freeing T
BF
<0002> pdch_ul_controller.c:329 PDCH(bts=0,trx=1,ts=6) Timeout for registered POLL (FN=1792743): TBF(TFI=31 TL
LI=0x7c31afb2 DIR=DL STATE=FLOW EGPRS)
<0008> tbf.cpp:629 TBF(TFI=31 TLLI=0x7c31afb2 DIR=DL STATE=FLOW EGPRS) poll timeout for FN=1792743, TS=6 (curr
 FN 1792743)
<0008> tbf.cpp:699 TBF(TFI=31 TLLI=0x7c31afb2 DIR=DL STATE=FLOW EGPRS) Timeout for polling PACKET DOWNLINK ACK
: |Assignment was on PACCH|Downlink ACK was received|
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=7) Expiring FN=1792743 but previous FN=1792739 is still re
served!
<0008> tbf.cpp:407 TBF(TFI=7 TLLI=0xa86f0e0e DIR=UL STATE=FLOW EGPRS) N3101 exceeded MAX (10)
<0002> gprs_rlcmac_ts_alloc.cpp:776 No USF available
<0008> tbf.cpp:746 TBF(TFI=0 TLLI=0x7e64c836 DIR=UL STATE=NULL EGPRS) Timeslot Allocation failed: trx = 1, sin
gle_slot = 0
<0008> tbf_ul.cpp:151 MS(TLLI=0x7e64c836, IMSI=618010111603467, TA=0, 12/12, DL) No PDCH resource
<0008> tbf.cpp:458 TBF(TFI=9 TLLI=0x8d2aa800 DIR=UL STATE=RELEASING EGPRS) T3169 timeout expired, freeing TBF
<0008> tbf.cpp:462 TBF(TFI=9 TLLI=0x8d2aa800 DIR=UL STATE=RELEASING EGPRS) T3169 timeout expired, freeing TBF:
 |Assignment was on PACCH|No uplink data received yet|
<0002> pdch_ul_controller.c:315 PDCH(bts=0,trx=1,ts=7) Expiring FN=1792760 but previous FN=1792747 is still re
served!
```

Backtrace Type 2

```
Program received signal SIGSEGV, Segmentation fault.
0x00007ffff6c92110 in osmo_fsm_state_name () from /usr/lib64/libosmocore.so.17
#0  0x00007ffff6c92110 in osmo_fsm_state_name () from /usr/lib64/libosmocore.so.17
#1  0x0000000000418fe3 in osmo_fsm_inst_state_name (fi=<optimized out>) at /root/builder/firmware-master/build
/rangesdmn-x86-64-core2/usr/include/osmocom/core/fsm.h:233
#2  gprs_rlcmac_tbf::state_name (this=0xe1fb80) at ./tbf.h:370
#3  gprs_rlcmac_tbf::name (this=0xe1fb80) at tbf.cpp:1070
#4  0x000000000041905a in tbf_name (tbf=<optimized out>) at tbf.cpp:1065
#5  0x000000000042ad01 in pdch_ulc_expire_fn (ulc=0x7bd690, fn=fn@entry=1792760) at pdch_ul_controller.c:327
#6  0x000000000040ff0b in pcu_rx_data_ind_pdtch (bts=bts@entry=0x7ad200, pdch=pdch@entry=0x7af720, data=data@e
ntry=0x7fffffffe326 "@\005\341\063\354\233", '+' <repeats 17 times>, len=<optimized out>, fn=1792760, meas=mea
s@entry=0x7fffffffe2a0) at pcu_l1_if.cpp:285
#7  0x0000000000410834 in pcu_rx_data_ind (data_ind=0x7fffffffe324, bts=0x7ad200) at pcu_l1_if.cpp:418
#8  pcu_rx (pcu_prim=pcu_prim@entry=0x7fffffffe320, pcu_prim_length=<optimized out>) at pcu_l1_if.cpp:992
#9  0x0000000000431399 in pcu_sock_read (bfd=<optimized out>) at osmobts_sock.c:156
#10 0x0000000000431585 in pcu_sock_cb (bfd=0x6974e0 <pcu_sock_state>, flags=1) at osmobts_sock.c:211
#11 0x00007ffff6c8e78c in ?? () from /usr/lib64/libosmocore.so.17
#12 0x00007ffff6c8e836 in osmo_select_main () from /usr/lib64/libosmocore.so.17
#13 0x0000000000406bf5 in main (argc=1, argv=0x7fffffffecd8) at pcu_main.cpp:329
$1 = {si_signo = 11, si_errno = 0, si_code = 1, _sifields = {_pad = {48, 0, 160, 0, 70288, 0, 50806128, 0, 816
916108, 32764, 951191690, 32604, 1, 0, 160, 0, 38817760, 0, 47792368, 0, 44, 0, 6622689, 0, 8149536, 0, 456560
64, 0}, _kill = {si_pid = 48, si_uid = 0}, _timer = {si_tid = 48, si_overrun = 0, si_sigval = {sival_int = 160
, sival_ptr = 0xa0}}, _rt = {si_pid = 48, si_uid = 0, si_sigval = {sival_int = 160, sival_ptr = 0xa0}}, _sigch
ld = {si_pid = 48, si_uid = 0, si_status = 160, si_utime = 301884661301248, si_stime = 218210658196389888}, _s
igfault = {si_addr = 0x30, _addr_lsb = 160, _addr_bnd = {_lower = 0x11290, _upper = 0x3073d70}}, _sigpoll = {s
i_band = 48, si_fd = 160}}}
```

#2 - 08/06/2021 05:12 PM - laforge

- Assignee set to neels

#3 - 08/09/2021 05:02 PM - neels

- Status changed from New to In Progress

The code where the SEGV is reported:

```
const char *tbf_name(const gprs_rlcmac_tbf *tbf)
{
        return tbf ? tbf->name() : "(no TBF)";
}
```

```
const char *gprs_rlcmac_tbf::name() const
{
        snprintf(m_name_buf, sizeof(m_name_buf) - 1,
                "TBF(TFI=%d TLLI=0x%08x DIR=%s STATE=%s%s)",
                m_tfi, tlli(),
                direction == GPRS_RLCMAC_UL_TBF ? "UL" : "DL",
                state_name(),
                is_egprs_enabled() ? " EGPRS" : ""
                );
        m_name_buf[sizeof(m_name_buf) - 1] = '\0';
        return m_name_buf;
}
```

AFAICT this cannot be a NULL dereference.

- tbf_name() checks against NULL tbf
- tlli() checks against a NULL m_ms
- state_name() uses osmo_fsm_inst_state_name() which is NULL safe
- state_fsm is a member struct and cannot be NULL
- is_gprs_enabled() merely returns a bool member

Since it's not a NULL deref, I guess it must be a use-after-free??

#4 - 08/09/2021 08:21 PM - neels

seems that the ulc->tree_root traversed in pdch_ulc_expire_fn() upon receiving a pdtch data ind
still points at a entry that has already been deallocated.

I'm pretty sure that the actual cause for the error happens way before the symptom shows:
at some point a tbf gets freed without calling tbf_free(), and it busts up pdch_ulc_expire_fn() some time later.

The reason is not trivial: tbf_free() properly calls tbf_unlink_pdch() that
removes the tbf entry via gprs_rlcmac_pdch::detach_tbf() and pdch_ulc_release_tbf()

Next checking whether:

- some error handling path frees a tbf in a different way,
- some parent talloc ctx might be freed and "pulls the carpet".

If I don't find any cause, we could add some strategic logging and analyse allocation and freeing next time it happens.

#5 - 09/15/2021 09:25 AM - laforge

- Assignee changed from neels to pespin

#6 - 09/15/2021 12:36 PM - pespin

- Status changed from In Progress to Feedback

- Assignee changed from pespin to iedemam

Same as #5205, let's ask @iedemam if he stills sees it with recent versions of osmo-pcu after FSM refactoring was merged (end of August).

#7 - 10/15/2021 03:49 PM - pespin

I believe this should be fixed in current osmo-pcu.git master b0aba591433c7c222980354537137241 72d1cfbc

Please @iedemam see if you can still reproduce.