OsmoPCU - Bug #4228

assert failed in osmo-pcu

10/16/2019 12:19 PM - pespin

Status:	Resolved	**Start date:**	10/16/2019
Priority:	Normal	**Due date:**	
Assignee:	pespin	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

```
20191016141542092 DL1IF <0001> /osmo-pcu/src/pcu_l1_if.cpp:402 RACH request received: sapi=1 qta=-
1, ra=117, fn=1596534, cur_fn=1596538, is_11bit=0
PayloadType = 1 | spare = 0 | R = 0 | MESSAGE_TYPE = 5 | Exist_ACCESS_TYPE = 1 | ACCESS_TYPE = 0 |
  : ID | Choice PacketResourceRequestID = 1 | u.TLLI = 0xe304f21f | : End ID | Exist_MS_Radio_Acce
ss_capability = 1 |  : MS_Radio_Access_capability | MS_RA_capability_value { | Choice MS_RA_capabi
lity_value_Choice = 3 | u.Content length = 66 | ptr = 0x5555556fb198 | offset = 4 | RF_Power_Capab
ility = 1 | Exist_A5_bits = 0 | ES_IND = 1 | PS = 1 | VGCS = 0 | VBS = 0 | Exist_Multislot_capabil
ity = 1 |  : Multislot_capability | Exist_HSCSD_multislot_class = 0 | Exist_GPRS_multislot_class =
 1 | GPRS_multislot_class = 12 | GPRS_Extended_Dynamic_Allocation_Capability = 1 | Exist_SM = 1 |
SMS_VALUE = 7 | SM_VALUE = 1 | Exist_ECSD_multislot_class = 0 | Exist_EGPRS_multislot_class = 1 |
EGPRS_multislot_class = 12 | EGPRS_Extended_Dynamic_Allocation_Capability = 1 | Exist_DTM_GPRS_mul
tislot_class = 1 | DTM_GPRS_multislot_class = 3 | Single_Slot_DTM = 0 |  : DTM_EGPRS_Params | Exis
t_DTM_EGPRS_multislot_class = 1 | DTM_EGPRS_multislot_class = 3 | : End DTM_EGPRS_Params | : End M
ultislot_capability | Exist_Eight_PSK_Power_Capability = 1 | Eight_PSK_Power_Capability = 2 | COMP
ACT_Interference_Measurement_Capability = 0 | Revision_Level_Indicator = 1 | UMTS_FDD_Radio_Access
_Technology_Capability = 0 | UMTS_384_TDD_Radio_Access_Technology_Capability = 0 | CDMA2000_Radio_
Access_Technology_Capability = 0 | UMTS_128_TDD_Radio_Access_Technology_Capability = 0 | GERAN_Fea
ture_Package_1 = 1 | Exist_Extended_DTM_multislot_class = 0 | Modulation_based_multislot_class_sup
port = 0 | Exist_HighMultislotCapability = 0 | Exist_GERAN_lu_ModeCapability = 0 | GMSK_MultislotP
owerProfile = 3 | EightPSK_MultislotProfile = 3 | MultipleTBF_Capability = 0 | DownlinkAdvancedRec
eiverPerformance = 1 | ExtendedRLC_MAC_ControlMessageSegmentionsCapability = 1 | DTM_EnhancementsC
apability = 1 | Exist_DTM_GPRS_HighMultislotClass = 0 | PS_HandoverCapability = 0 | MS_RA_capabili
ty_value } | : End MS_Radio_Access_capability |  : Channel_Request_Description | PEAK_THROUGHPUT_C
LASS = 6 | RADIO_PRIORITY = 0 | RLC_MODE = 0 | LLC_PDU_TYPE = 1 | RLC_OCTET_COUNT = 82 | : End Cha
nnel_Request_Description | Exist_CHANGE_MARK = 0 | C_VALUE = 44 | Exist_SIGN_VAR = 0 | Slot | Exis
t = 0 | Slot | Exist = 0 | Slot | Exist = 0 | Slot | Exist = 0 | Slot | Exist = 0 | Slot | Exist =
 0 | Slot | Exist = 0 | Slot | Exist = 0 | Exist_AdditionsR99 = 1 |  : AdditionsR99 | Exist_EGPRS_
BEP_LinkQualityMeasurements = 0 | Exist_EGPRS_TimeslotLinkQualityMeasurements = 0 | Exist_PFI = 0
| MS_RAC_AdditionalInformationAvailable = 0 | RetransmissionOfPRR = 0 | : End AdditionsR99 | Paddi
ng = 0|43|
20191016141542489 DRLCMAC <0002> /osmo-pcu/src/pdch.cpp:596 MS supports EGPRS multislot class 12.
20191016141542489 DTBF <0008> /osmo-pcu/src/tbf.cpp:989 Allocating UL TBF: MS_CLASS=12/12
20191016141542489 DTBF <0008> /osmo-pcu/src/tbf.cpp:541 TBF(TFI=0 TLLI=0x00000000 DIR=UL STATE=NUL
L) Setting Control TS 6
20191016141542489 DTBF <0008> /osmo-pcu/src/tbf.cpp:945 TBF(TFI=0 TLLI=0xe304f21f DIR=UL STATE=NUL
L) Allocated: trx = 0, ul_slots = 40, dl_slots = 00
20191016141542491 DTBF <0008> /osmo-pcu/src/tbf.cpp:1359 TBF(TFI=0 TLLI=0xe304f21f DIR=UL STATE=AS
SIGN) start Packet Uplink Assignment (PACCH)
MESSAGE_TYPE = 10 | PAGE_MODE = 0 | Exist_PERSISTENCE_LEVEL = 0 |  : ID | Choice PacketUplinkID =
2 | u.TLLI = 0xe304f21f | : End ID | u.PUA_GPRS_Struct = 0 |  : u.PUA_GPRS_Struct | CHANNEL_CODING
_COMMAND = 1 | TLLI_BLOCK_CHANNEL_CODING = 1 |  : Packet_Timing_Advance | Exist_TIMING_ADVANCE_VAL
UE = 1 | TIMING_ADVANCE_VALUE = 0 | Exist_IndexAndtimeSlot = 0 | : End Packet_Timing_Advance | Exi
st_Frequency_Parameters = 1 |  : Frequency_Parameters | TSC = 7 | u.ARFCN = 0 | u.ARFCN = 870 | :
End Frequency_Parameters | u.Dynamic_Allocation = 1 |  : u.Dynamic_Allocation | Extended_Dynamic_A
llocation = 0 | Exist_P0 = 0 | USF_GRANULARITY = 0 | Exist_UPLINK_TFI_ASSIGNMENT = 1 | UPLINK_TFI_
ASSIGNMENT = 0 | Exist_RLC_DATA_BLOCKS_GRANTED = 0 | Exist_TBF_Starting_Time = 0 | u.Timeslot_Allo
cation = 0 | u.Timeslot_Allocation | Exist = 0 | u.Timeslot_Allocation | Exist = 0 | u.Timeslot_Al
location | Exist = 0 | u.Timeslot_Allocation | Exist = 0 | u.Timeslot_Allocation | Exist = 0 | u.T
imeslot_Allocation | Exist = 0 | u.Timeslot_Allocation | Exist = 1 | USF_TN = 0 | u.Timeslot_Alloc
ation | Exist = 0 |  : End u.Dynamic_Allocation | Exist_AdditionsR99 = 0 |  : End u.PUA_GPRS_Struc
t | Padding = 43|43|43|43|43|43|43|43|43|43|
```

```
20191016141542491 DTBFDL <0009> /osmo-pcu/src/tbf.cpp:782 TBF(TFI=0 TLLI=0xe304f21f DIR=UL STATE=A
SSIGN) Scheduled UL Assignment polling on PACCH (FN=1596664, TS=7)
PayloadType = 1 | spare = 0 | R = 0 | MESSAGE_TYPE = 1 | TLLI = 0xe304f21f | CTRL_ACK = 3 | Exist_
AdditionsR5 = 0 | Padding = 43|43|43|43|43|43|43|43|43|43|43|43|43|43|43|43|
20191016141542710 DTBF <0008> /osmo-pcu/src/tbf.cpp:544 TBF(TFI=0 TLLI=0xe304f21f DIR=UL STATE=FLO
W) Changing Control TS 6
20191016141542931 DBSSGP <000c> /osmo-pcu/src/tbf_ul.cpp:404 LLC [PCU -> SGSN] TBF(TFI=0 TLLI=0xe3
04f21f DIR=UL STATE=FLOW) len=82
20191016141542963 DBSSGP <000c> /osmo-pcu/src/gprs_bssgp_pcu.cpp:181  P-TMSI = e304f21f
20191016141542963 DRLCMAC <0002> /osmo-pcu/src/gprs_rlcmac.cpp:34 TX: [PCU -> BTS] Paging Request
(CCCH)
Assert failed sizeof(data) >= PAGING_GROUP_LEN + 1 + block->data_len /osmo-pcu/src/pcu_l1_if.cpp:2
40
backtrace() returned 21 addresses
/lib/libosmocore.so.12(osmo_generate_backtrace+0x18) [0x7ffff7d05575]
/lib/libosmocore.so.12(+0x1e27d) [0x7ffff7d0527d]
/lib/libosmocore.so.12(osmo_panic+0xdc) [0x7ffff7d0535e]
/bin/osmo-pcu(+0x29c66) [0x55555557dc66]
/bin/osmo-pcu(+0x22c8f) [0x555555576c8f]
/bin/osmo-pcu(+0x2045e) [0x55555557445e]
/bin/osmo-pcu(+0x209bb) [0x5555555749bb]
/bin/osmo-pcu(+0x21093) [0x555555575093]
/bin/osmo-pcu(+0x213b6) [0x5555555753b6]
/lib/libosmogb.so.9(+0x8c78) [0x7ffff7fa5c78]
/lib/libosmogb.so.9(+0xb0c3) [0x7ffff7fa80c3]
/lib/libosmogb.so.9(gprs_ns_rcvmsg+0xe1) [0x7ffff7fa734e]
/lib/libosmogb.so.9(+0xbc40) [0x7ffff7fa8c40]
/lib/libosmogb.so.9(+0xbd17) [0x7ffff7fa8d17]
/lib/libosmocore.so.12(osmo_fd_disp_fds+0x26b) [0x7ffff7cf37f6]
/lib/libosmocore.so.12(+0xc9cd) [0x7ffff7cf39cd]
/lib/libosmocore.so.12(osmo_select_main+0x15) [0x7ffff7cf39f8]
/bin/osmo-pcu(+0x1e4e8) [0x5555555724e8]
/usr/lib/libc.so.6(__libc_start_main+0xf3) [0x7ffff77c2ee3]
/bin/osmo-pcu(+0x1da6e) [0x555555571a6e]
```

Proably related to osmo-pcu f681f07cd0c2d5232d6cf3c1da2192cc7bc9c576..d752d7cebe51bd690d31147ef5173c3f33ec7f41

History

#1 - 10/16/2019 12:22 PM - pespin

```
(gdb) print block->data_len
$1 = 23
```

#2 - 10/16/2019 12:28 PM - pespin

```
(gdb) bt full
#0  0x00007ffff77d1755 in raise () from /usr/lib/libc.so.6
No symbol table info available.
#1  0x00007ffff77bc851 in abort () from /usr/lib/libc.so.6
No symbol table info available.
#2  0x00007ffff7d05282 in osmo_panic_default (
    fmt=0x5555555b71d7 "Assert failed %s %s:%d\n", args=0x7fffffffba90)
    at /git/libosmocore/src/panic.c:49
No locals.
#3  0x00007ffff7d0535e in osmo_panic (
    fmt=0x5555555b71d7 "Assert failed %s %s:%d\n")
    at /git/libosmocore/src/panic.c:84
        args = {{gp_offset = 32, fp_offset = 48,
            overflow_arg_area = 0x7fffffffbb70,
            reg_save_area = 0x7fffffffbab0}}
#4  0x000055555557dc66 in pcu_l1if_tx_pch (block=0x5555556f5e70, plen=9,
    imsi=0x7fffffffbc5c "256")
    at /git/osmo-pcu/src/pcu_l1_if.cpp:240
        bts = 0x5555555f6dc8 <s_bts+8>
        data = "256UUU\000\000p^oUUU\000\000`\340bUUU\000\000\v"
#5  0x0000555555576c8f in gprs_rlcmac_paging_request (
    ptmsi=0x55555571b15a "\315}g\200", ptmsi_len=4,
```

```
    imsi=0x7fffffffbc50 "901700000015256")
    at /git/osmo-pcu/src/gprs_rlcmac.cpp:38
--Type <RET> for more, q to quit, c to continue without paging--
        paging_request = 0x5555556f5e70
        plen = 9
#6  0x000055555557445e in gprs_bssgp_pcu_rx_paging_ps (msg=0x55555571b0a0,
    tp=0x7fffffffbd10)
    at /git/osmo-pcu/src/gprs_bssgp_pcu.cpp:201
        imsi = "901700000015256"
        ptmsi = 0x55555571b15a "\315}g\200"
        ptmsi_len = 4
        rc = 16
#7  0x00005555555749bb in gprs_bssgp_pcu_rx_sign (msg=0x55555571b0a0,
    tp=0x7fffffffbd10, bctx=0x0)
    at /git/osmo-pcu/src/gprs_bssgp_pcu.cpp:305
        bgph = 0x55555571b140
        pdu_type = BSSGP_PDUT_PAGING_PS
        rc = 0
        bvci = -1
#8  0x0000555555575093 in gprs_bssgp_pcu_rcvmsg (msg=0x55555571b0a0)
    at /git/osmo-pcu/src/gprs_bssgp_pcu.cpp:430
        bgph = 0x55555571b140
        budh = 0x55555571b140
        tp = {lv = {{len = 0, val = 0x0}, {len = 0, val = 0x0}, {len = 0,
              val = 0x0}, {len = 0, val = 0x0}, {len = 2,
              val = 0x55555571b151 "\a\b\030\203"}, {len = 0, val = 0x0}, {
--Type <RET> for more, q to quit, c to continue without paging--
              len = 0, val = 0x0}, {len = 0, val = 0x0}, {len = 0, val = 0x0},
            {len = 0, val = 0x0}, {len = 2, val = 0x55555571b14d "\n"}, {
              len = 0, val = 0x0}, {len = 0, val = 0x0}, {len = 8,
              val = 0x55555571b143 "\231\020\a"}, {len = 0, val = 0x0}, {
              len = 0, val = 0x0}, {len = 0, val = 0x0}, {len = 0, val = 0x0},
            {len = 0, val = 0x0}, {len = 0, val = 0x0}, {len = 0, val = 0x0}, {
              len = 0, val = 0x0}, {len = 0, val = 0x0}, {len = 0, val = 0x0},
            {len = 3, val = 0x55555571b155 ""}, {len = 0, val = 0x0}, {
              len = 0, val = 0x0}, {len = 0, val = 0x0}, {len = 0, val = 0x0},
            {len = 0, val = 0x0}, {len = 0, val = 0x0}, {len = 0, val = 0x0}, {
              len = 4, val = 0x55555571b15a "\315}g\200"}, {len = 0,
              val = 0x0} <repeats 223 times>}}
        pdu_type = BSSGP_PDUT_PAGING_PS
        cause = BSSGP_CAUSE_OML_INTERV
        ns_bvci = 0
        nsei = 1800
        data_len = 29
        rc = 5
        bctx = 0x0
#9  0x00005555555753b6 in gprs_bssgp_ns_cb (event=GPRS_NS_EVT_UNIT_DATA,
    nsvc=0x555555661e10, msg=0x55555571b0a0, bvci=0)
    at /git/osmo-pcu/src/gprs_bssgp_pcu.cpp:514
        rc = 0
--Type <RET> for more, q to quit, c to continue without paging--
#10 0x00007ffff7fa5c78 in gprs_ns_rx_unitdata (nsvc=0x555555661e10,
    msg=0x55555571b0a0)
    at /git/libosmocore/src/gb/gprs_ns.c:1143
        nsh = 0x55555571b13c
        bvci = 0
#11 0x00007ffff7fa80c3 in gprs_ns_process_msg (nsi=0x55555567e180,
    msg=0x55555571b0a0, nsvc=0x7fffffffde28)
    at /git/libosmocore/src/gb/gprs_ns.c:1778
        nsh = 0x55555571b13c
        tp = {lv = {{len = 0, val = 0x0}, {len = 52768,
              val = 0x7ffff7d02477 <should_log_to_target+212> "\205\300\017\225\300\353\005\270\001"}, {len =
5,
              val = 0x5555556f7c70 "\340\331\322\367\377\177"}, {len = 52896,
              val = 0x55555562e660 "p|oUUU"}, {len = 52896,
              val = 0x7ffff7d025df <osmo_vlogp+346> "\220H\213E\370dH3\004%("}, {len = 30224, val = 0x7fffffff
cee0 '+' <repeats 17 times>}, {len = 43629,
              val = 0xd000000001 <error: Cannot access memory at address 0xd000000001>}, {len = 43640,
              val = 0x5 <error: Cannot access memory at address 0x5>}, {
              len = 19524,
              val = 0x7ffff7d2d9e0 <osmo_log_target_list> "`\346bUUU"}, {
              len = 58976,
              val = 0x7ffff7d2d9e0 <osmo_log_target_list> "`\346bUUU"}, {
--Type <RET> for more, q to quit, c to continue without paging--
              len = 48, val = 0x7fffffffcfd0 "6f[UUU"}, {len = 52992,
```

```
              val = 0x7ffff7d04f92 <gsmtap_sink_fd_cb+91> "\211\205\354\357\377\377\203\275\354\357\377\377"},
 {len = 53168, val = 0x55555567d868 ""}, {
              len = 52960,
              val = 0x276e69646e <error: Cannot access memory at address 0x276e69646e>}, {len = 1026,
              val = 0xb12751100 <error: Cannot access memory at address 0xb12751100>}, {len = 37959,
              val = 0x2b2b2b2b2b2b2b2b <error: Cannot access memory at address 0x2b2b2b2b2b2b2b2b>}, {len = 11
051,
              val = 0x2b2b2b2b2b2b2b2b <error: Cannot access memory at address 0x2b2b2b2b2b2b2b2b>}, {len = 43
,
              val = 0x459a742196b3b900 <error: Cannot access memory at address 0x459a742196b3b900>}, {len = 11
051,
              val = 0xb35c6 <error: Cannot access memory at address 0xb35c6>},
            {len = 2,
              val = 0x100000000e <error: Cannot access memory at address 0x100000000e>}, {len = 9,
              val = 0x12000000003 <error: Cannot access memory at address 0x12000000003>}, {len = 1,
              val = 0x6600001c20 <error: Cannot access memory at address 0x6600001c20>}, {len = 30224,
              val = 0x100001c01 <error: Cannot access memory at address 0x100001--Type <RET> for more, q to qu
it, c to continue without paging--
c01>}, {len = 53120,
              val = 0x7ffff7cf63d8 <bitvec_get_bit_pos+76> "\210E\367H\213E\350H\213P\b\213E\370H\001\320\017\
266"}, {len = 5, val = 0x55555562e660 "p|oUUU"},
            {len = 31856, val = 0x7ffff7d2dbc0 <log_context> "\020\036fUUU"}, {
              len = 0, val = 0x0}, {len = 53184,
              val = 0x7ffff7d02477 <should_log_to_target+212> "\205\300\017\225\300\353\005\270\001"}, {len =
5,
              val = 0x5555556f7c70 "\340\331\322\367\377\177"}, {len = 53312,
              val = 0x55555562e660 "p|oUUU"}, {len = 53312,
              val = 0x7ffff7d025df <osmo_vlogp+346> "\220H\213E\370dH3\004%("}, {len = 26166, val = 0x7fffffff
d080 "0"}, {len = 43968,
              val = 0x1d700000001 <error: Cannot access memory at address 0x1d700000001>}, {len = 43640,
              val = 0x5 <error: Cannot access memory at address 0x5>}, {
              len = 27963,
              val = 0x7ffff7d2d9e0 <osmo_log_target_list> "`\346bUUU"}, {
              len = 58976,
              val = 0x7ffff7d2d9e0 <osmo_log_target_list> "`\346bUUU"}, {
              len = 48, val = 0x7fffffffd168 ""}, {len = 0,
              val = 0x459a742196b3b900 <error: Cannot access memory at address 0x459a742196b3b900>}, {len = 53
584, val = 0x5555555bb109 ""}, {len = 54752,
              val = 0x7fffffffd600 "\005"}, {len = 45305,
              val = 0x7fffffffd780 "\003"}, {len = 20672,
--Type <RET> for more, q to quit, c to continue without paging--
              val = 0x7ffff77ffa88 <__vfprintf_internal+2024> "H\213\225H\373\377\377H\211\321H)\331H9\310\017
\205\302\372\377\377D\213\215\020\373\377\377\271\377\377\377\177D)\311Hc\311H9\310\017\217\327\374\377\377A\0
01\301\200:"}, {
              len = 48,
              val = 0x7fff00000000 <error: Cannot access memory at address 0x7fff00000000>}, {len = 53408, val
 = 0x0}, {len = 7,
              val = 0x7fff00000000 <error: Cannot access memory at address 0x7fff00000000>}, {len = 1,
              val = 0x7 <error: Cannot access memory at address 0x7>}, {
              len = 20672, val = 0x5555555bcb98 ")"}, {len = 54880,
              val = 0x7fffffffd680 "\001\200\255\373\060"}, {len = 52080,
              val = 0x7fffffffd800 "\006"}, {len = 20672,
              val = 0x7ffff77ffa88 <__vfprintf_internal+2024> "H\213\225H\373\377\377H\211\321H)\331H9\310\017
\205\302\372\377\377D\213\215\020\373\377\377\271\377\377\377\177D)\311Hc\311H9\310\017\217\327\374\377\377A\0
01\301\200:"}, {
              len = 18368,
              val = 0x1100000000 <error: Cannot access memory at address 0x1100000000>}, {len = 1, val = 0x0},
 {len = 0,
              val = 0x555500000000 <error: Cannot access memory at address 0x555500000000>}, {len = 65535, val
 = 0x0}, {len = 43, val = 0x5555555bb21c ""}, {
              len = 0, val = 0x5555555bb200 "h is already set.\n"}, {len = 0,
              val = 0x0}, {len = 43,
              val = 0x200000005 <error: Cannot access memory at address 0x200000--Type <RET> for more, q to qu
it, c to continue without paging--
005>}, {len = 18368,
              val = 0xd68 <error: Cannot access memory at address 0xd68>}, {
              len = 52088, val = 0x0}, {len = 1, val = 0x5555555bcb99 ""}, {
              len = 0,
              val = 0x555500000000 <error: Cannot access memory at address 0x555500000000>}, {len = 65535, val
 = 0x7fffffffd328 ""}, {len = 43,
              val = 0xffffffffffffffff <error: Cannot access memory at address 0xffffffffffffffff>}, {len = 0,
              val = 0x7fffffffd940 "\240\331\377\377\377\177"}, {len = 55568,
              val = 0x1 <error: Cannot access memory at address 0x1>}, {
              len = 16,
              val = 0xffffffff <error: Cannot access memory at address 0xffffffff>}, {len = 0,
```

```
              val = 0x3000000018 <error: Cannot access memory at address 0x3000000018>}, {len = 55520, val = 0
x7fffffffd820 "0\331\377\377\377\177"}, {
              len = 53824, val = 0x7ffff791f648 <dot> "."}, {len = 1,
              val = 0x0}, {len = 55592, val = 0x5555555bcb98 ")"}, {
              len = 55280, val = 0x7fffffffd810 ""}, {len = 52080,
              val = 0x7fffffffd990 "p|oUUU"}, {len = 20672,
              val = 0x7ffff77ffa88 <__vfprintf_internal+2024> "H\213\225H\373\377\377H\211\321H)\331H9\310\017
\205\302\372\377\377D\213\215\020\373\377\377\271\377\377\377\177D)\311Hc\311H9\310\017\217\327\374\377\377A\0
01\301\200:"}, {
              len = 52080,
--Type <RET> for more, q to quit, c to continue without paging--
              val = 0x1100000000 <error: Cannot access memory at address 0x1100000000>}, {len = 1, val = 0x0},
 {len = 0,
              val = 0x1100000000 <error: Cannot access memory at address 0x1100000000>}, {len = 65535, val = 0
x0}, {len = 43, val = 0x5555555bb21c ""}, {
              len = 0, val = 0x5555555bb200 "h is already set.\n"}, {len = 0,
              val = 0x0}, {len = 43,
              val = 0x200000005 <error: Cannot access memory at address 0x200000005>}, {len = 18368,
              val = 0xd68 <error: Cannot access memory at address 0xd68>}, {
              len = 52088, val = 0x0}, {len = 18368, val = 0x5555555bcb99 ""},
            {len = 52088, val = 0x0}, {len = 54208, val = 0x5555555bcb99 ""}, {
              len = 54384,
              val = 0x7ffff7d027b6 <logp2+207> "H\203\304\020\220H\213\205H\377\377\377dH3\004%("}, {len = 541
76, val = 0x7fffffffda40 "\\\255oUUU"}, {
              len = 43629,
              val = 0x3d000000001 <error: Cannot access memory at address 0x3d000000001>}, {len = 43640,
              val = 0x5 <error: Cannot access memory at address 0x5>}, {
              len = 48,
              val = 0x3000000018 <error: Cannot access memory at address 0x3000000018>}, {len = 55920, val = 0
x7fffffffd9b0 "\340\331\377\377\377\177"}, {
              len = 54256,
              val = 0x3000000018 <error: Cannot access memory at address 0x30000--Type <RET> for more, q to qu
it, c to continue without paging--
00018>}, {len = 55952, val = 0x7fffffffd9d0 "\017\001"}, {len = 43640,
              val = 0x5 <error: Cannot access memory at address 0x5>}, {
              len = 48,
              val = 0x67ffffd4d0 <error: Cannot access memory at address 0x67ffffd4d0>}, {len = 54288,
              val = 0x196b3b900 <error: Cannot access memory at address 0x196b3b900>}, {len = 54336,
              val = 0x7ffff7cf63d8 <bitvec_get_bit_pos+76> "\210E\367H\213E\350H\213P\b\213E\370H\001\320\017\
266"}, {len = 5, val = 0x55555562e660 "p|oUUU"},
            {len = 31856,
              val = 0x55555562e770 "\003\001\003\001\005\001\005\001\005\001\005\001\005\001\003\001\003\001\0
03\001\003\001\003\001\003\001\005\001\005\001\005\001\005\001\005\001\005\001\005\001\005\001\005\001\005\001
\005\001\005\001\005\001\005\001\005\001\005\001\005\001\005\001\005\001"}, {len = 54400,
              val = 0x7ffff7d03316 <log_check_level+151> "\270\001"}, {
              len = 54400,
              val = 0x5 <error: Cannot access memory at address 0x5>}, {
              len = 56096, val = 0x55555562e660 "p|oUUU"}, {len = 54816,
              val = 0x5555555aea85
     <csnStreamDecoder(csnStream_t*, CSN_DESCR const*, bitvec*, unsigned int&, void*)+11303> "H\203\304\020\20
3\205\b\377\377\377\001\200\275\257\376\377\377"}, {len = 17831, val = 0x0}, {len = 54480, val = 0x55555571b0f
9 "\a"}, {
              len = 56096, val = 0x5555556f5e70 "N"}, {len = 4048,
--Type <RET> for more, q to quit, c to continue without paging--
              val = 0x7fffffffd744 "P"}, {len = 98,
              val = 0x7fff01d2d9e0 <error: Cannot access memory at address 0x7fff01d2d9e0>}, {len = 58976,
              val = 0x7ffff7d2d9e0 <osmo_log_target_list> "`\346bUUU"}, {
              len = 48, val = 0x7fffffffd628 ""}, {len = 54624,
              val = 0x459a742196b3b900 <error: Cannot access memory at address 0x459a742196b3b900>}, {len = 54
800,
              val = 0x7ffff7d027b6 <logp2+207> "H\203\304\020\220H\213\205H\377\377\377dH3\004%("}, {len = 545
92,
              val = 0x7fff01d2d9e0 <error: Cannot access memory at address 0x7fff01d2d9e0>}, {len = 43784,
              val = 0x33f00000068 <error: Cannot access memory at address 0x33f00000068>}, {len = 43640,
              val = 0x5 <error: Cannot access memory at address 0x5>}, {
              len = 48, val = 0x7fffffffd620 "cd7d6780"}, {len = 45305,
              val = 0x459a742196b3b900 <error: Cannot access memory at address 0x459a742196b3b900>}, {len = 54
672, val = 0x7fffffffd660 "äqUUU"}, {
              len = 43980,
              val = 0x1fc00000080 <error: Cannot access memory at address 0x1fc00000080>}, {len = 43640,
              val = 0x5 <error: Cannot access memory at address 0x5>}, {
              len = 48,
              val = 0x5cffffd600 <error: Cannot access memory at address 0x5cfff--Type <RET> for more, q to qu
it, c to continue without paging--
fd600>}, {len = 55527,
```

```
              val = 0x196b3b903 <error: Cannot access memory at address 0x196b3b903>}, {len = 54752,
              val = 0x7ffff7cf63d8 <bitvec_get_bit_pos+76> "\210E\367H\213E\350H\213P\b\213E\370H\001\320\017\
266"}, {len = 5, val = 0x55555562e660 "p|oUUU"},
            {len = 31856, val = 0x7ffff7d2dbc0 <log_context> "\020\036fUUU"}, {
              len = 0, val = 0x0}, {len = 54816,
              val = 0x7ffff7d02477 <should_log_to_target+212> "\205\300\017\225\300\353\005\270\001"}, {len =
5,
              val = 0x5555556f7c70 "\340\331\322\367\377\177"}, {len = 54944,
              val = 0x7fffffffd680 "\001\200\255\373\060"}, {len = 25699,
              val = 0x459a742196b3b900 <error: Cannot access memory at address 0x459a742196b3b900>}, {len = 40
915, val = 0x0}, {len = 58,
              val = 0x7fffffffd680 "\001\200\255\373\060"}, {len = 52080,
              val = 0x7fffffffd800 "\006"}, {len = 40915,
              val = 0x7ffff7812c5a <__vsnprintf_internal+170> "L\213L$\bL9L$Ht\bH\213T$8\306\002"}, {len = 589
76,
              val = 0x7fffffffd770 "\240\327\377\377\377\177"}, {len = 32769,
              val = 0x555555719fd3 "TBF(TFI=0 TLLI=0xcd7d6780 DIR=UL STATE=FLOW)"}, {len = 40915,
              val = 0x555555719fd3 "TBF(TFI=0 TLLI=0xcd7d6780 DIR=UL STATE=FLOW)"}, {len = 40915, val = 0x5555
55719fff ""}, {len = 40973,
              val = 0x555555719fd3 "TBF(TFI=0 TLLI=0xcd7d6780 DIR=UL STATE=FLOW)--Type <RET> for more, q to qu
it, c to continue without paging--
"}, {len = 40973, val = 0x0}, {len = 0, val = 0x0}, {len = 0, val = 0x0}, {
              len = 55040,
              val = 0x459a742196b3b900 <error: Cannot access memory at address 0x459a742196b3b900>}, {len = 0,
 val = 0x0}, {len = 32769,
              val = 0x555555719fd3 "TBF(TFI=0 TLLI=0xcd7d6780 DIR=UL STATE=FLOW)"}, {len = 65535, val = 0x0},
{len = 40915,
              val = 0x6855719fff <error: Cannot access memory at address 0x6855719fff>}, {len = 65535,
              val = 0x100000007 <error: Cannot access memory at address 0x100000007>}, {len = 31856, val = 0x7
ffff7d2dbc0 <log_context> "\020\036fUUU"}, {
              len = 0, val = 0x0}, {len = 55200,
              val = 0x459a742196b3b900 <error: Cannot access memory at address 0x459a742196b3b900>}, {len = 3,
 val = 0x55555569aff0 ""}, {len = 44944,
              val = 0x7ffff7d21308 "/git/libosmocore/src/msgb.c:123"}, {len = 44944, val = 0x0}, {len = 0,
              val = 0x7ffff7cd5144 <_talloc_free+612> "H\203\304(1\300[]A\\A]A^A_\303\017\037"}, {len = 53787,
              val = 0x19400000000 <error: Cannot access memory at address 0x19400000000>}, {len = 52504,
              val = 0xc00000003 <error: Cannot access memory at address 0xc00000003>}, {len = 47889, val = 0x5
555556fa748 'B' <repeats 200 times>...}, {
              len = 55344, val = 0x5555555f6dc0 <s_bts> "\342t\021"}, {
              len = 6, val = 0x0}, {len = 0,
--Type <RET> for more, q to quit, c to continue without paging--
              val = 0x7ffff7cf44d2 <msgb_free+31> "\220\311\303UH\211\345H\203\354\020H\211}\370H\211u\360H\21
3E\360H\213U\370H\211\326H\211\307\350\331\372\377\377\220\311\303UH\211\345H\203\354\030H\211}\350H\213E\350H
\211\307\350R\373\377\377\205\300t\a\270"}, {len = 55600, val = 0x55555569aff0 ""}, {len = 55408,
              val = 0x7ffff7fa8ce6 <nsip_sendmsg+111> "\213E\354\311\303UH\211\345H\203\354 H\211}\350\211u\34
4\307", <incomplete sequence \374>}, {
              len = 45040, val = 0x555555661e10 "\210\341gUUU"}, {len = 55408,
              val = 0x61f7fa3071 <error: Cannot access memory at address 0x61f7fa3071>}, {len = 57728, val = 0
x555555661ebc "\002"}, {len = 55456,
              val = 0x7ffff7fa3ccc <gprs_ns_tx+356> "\211E\364\203", <incomplete sequence \364>}, {len = 45040
, val = 0x555555661e10 "\210\341gUUU"}, {
              len = 7696, val = 0x55555569b096 ""}, {len = 55520,
              val = 0x7ffff7fa5bc7 <gprs_ns_sendmsg+573> "\311\303UH\211\345H\203\354 H\211}\350H\211u\340H\21
3E\340H\213@(H\211E\370H\213E\350\213@\034\203\340\001\205\300t\037H\213U\340H\213E\350H\211
              val = 0x55555567e180 "\203SWUUU"}, {len = 55520,
              val = 0x7fff070833aa <error: Cannot access memory at address 0x7fff070833aa>}, {len = 7696, val
= 0x55555569b096 ""}, {len = 55616,
              val = 0x7ffff7fb4af6 <bssgp_tx_ul_ud+375> "H\213u\370dH34%("}, {
              len = 45040, val = 0x7fffffffd985 ""}, {len = 53825,
              val = 0x5555556f83e0 "p\f\374\367\377\177"}, {len = 55616,
              val = 0x55555569aff0 ""}, {len = 45210,
              val = 0x5555584ffb <error: Cannot access memory at address 0x55555--Type <RET> for more, q to qu
it, c to continue without paging--
84ffb>}, {len = 62514, val = 0x5555556fa748 'B' <repeats 200 times>...}, {
              len = 55712, val = 0x55555558d047
    <gprs_rlcmac_ul_tbf::snd_ul_ud()+445> "\270"}, {len = 31856,
              val = 0x7ffff7d2dbc0 <log_context> "\020\036fUUU"}, {len = 7696,
              val = 0x0}, {len = 55712,
              val = 0x7ffff7d02477 <should_log_to_target+212> "\205\300\017\225\300\353\005\270\001"}, {len =
1,
              val = 0x5555556f7c70 "\340\331\322\367\377\177"}, {len = 31856,
              val = 0x55555562e660 "p|oUUU"}, {len = 55776,
              val = 0x7ffff7d03332 <log_check_level+179> "\270"}, {
              len = 55776,
              val = 0x800000001 <error: Cannot access memory at address 0x800000001>}, {len = 1, val = 0x1 <er
```

```
ror: Cannot access memory at address 0x1>}, {
              len = 271, val = 0x555555630910 ""}, {len = 2224,
              val = 0x7ffff7cd7b52 <talloc_named_const+578> "H\213\064$H\213T$\bH\205\300H\211\303\017\204\345
\376\377\377\213\005\233", <incomplete sequence \304>}, {len = 175, val = 0x7ffff7d236b4 "gsmtap_tx"}, {len =
387,
              val = 0x1 <error: Cannot access memory at address 0x1>}, {
              len = 55920,
              val = 0x7 <error: Cannot access memory at address 0x7>}, {
              len = 7, val = 0x0}, {len = 0,
              val = 0x7ffff7cf442b <msgb_alloc_c+174> "H\213E\370\017\267U\344f\211PhH\213E\370f\307@j"}, {len
 = 44380, val = 0x55555567d840 "@\330gUUU"}, {
--Type <RET> for more, q to quit, c to continue without paging--
              len = 55360, val = 0x55555567c290 ""}...}}
        rc = 0
#12 0x00007ffff7fa734e in gprs_ns_rcvmsg (nsi=0x55555567e180,
    msg=0x55555571b0a0, saddr=0x7fffffffde80, ll=GPRS_NS_LL_UDP)
    at /git/libosmocore/src/gb/gprs_ns.c:1527
        nsvc = 0x555555661e10
        rc = 0
#13 0x00007ffff7fa8c40 in handle_nsip_read (bfd=0x55555567e1b0)
    at /git/libosmocore/src/gb/gprs_ns.c:1993
        error = 0
        saddr = {sin_family = 2, sin_port = 55385, sin_addr = {
            s_addr = 18786496}, sin_zero = "\000\000\000\000\000\000\000"}
        nsi = 0x55555567e180
        msg = 0x55555571b0a0
#14 0x00007ffff7fa8d17 in nsip_fd_cb (bfd=0x55555567e1b0, what=1)
    at /git/libosmocore/src/gb/gprs_ns.c:2026
        rc = 0
#15 0x00007ffff7cf37f6 in osmo_fd_disp_fds (_rset=0x7fffffffdfa0,
    _wset=0x7fffffffe020, _eset=0x7fffffffe0a0)
    at /git/libosmocore/src/select.c:225
        flags = 1
        ufd = 0x55555567e1b0
        tmp = 0x7ffff7d2d990 <osmo_fds>
--Type <RET> for more, q to quit, c to continue without paging--
        work = 1
        readset = 0x7fffffffdfa0
        writeset = 0x7fffffffe020
        exceptset = 0x7fffffffe0a0
#16 0x00007ffff7cf39cd in _osmo_select_main (polling=0)
    at /git/libosmocore/src/select.c:263
        readset = {__fds_bits = {0 <repeats 16 times>}}
        writeset = {__fds_bits = {0 <repeats 16 times>}}
        exceptset = {__fds_bits = {0 <repeats 16 times>}}
        rc = 1
        no_time = {tv_sec = 0, tv_usec = 0}
#17 0x00007ffff7cf39f8 in osmo_select_main (polling=0)
    at /git/libosmocore/src/select.c:272
        rc = 1167750177
#18 0x00005555555724e8 in main (argc=5, argv=0x7fffffffe288)
    at /git/osmo-pcu/src/pcu_main.cpp:354
        param = {sched_priority = 1431771712}
        bts = 0x5555555f6dc8 <s_bts+8>
        rc = 0
```

#3 - 10/16/2019 12:44 PM - pespin

- Status changed from New to Feedback

- % Done changed from 0 to 90

Should be fixed by:
https://gerrit.osmocom.org/c/osmo-pcu/+/15799 Fix assertion hit upon CCCH Paging Request

#4 - 11/07/2019 10:50 PM - pespin

- Status changed from Feedback to Resolved

- % Done changed from 90 to 100