OsmoPCU - Bug #4973
NULL m_dl_egprs_ctrs passed to rate_ctr_add()
01/25/2021 12:01 AM - keith

Status: Resolved
Priority: Normal
Assignee: pespin
Category: Spec Reference:

Description
(gdb) bt
#0 0xb6eddda0 in rate_ctr_add () from /usr/lib/libosmocore.so.16
#1 0x0002f274 in gprs_rlcmac_dl_tbf::create_dl_acked_block (this=this@entry=0x5da078, fn=338684, fn@entry=124215, ts=ts@entry=7 'a', index=0, index@entry=79, index2=-1)
   at /usr/src/debug/osmo-pcu/0.8.0+gitAUTOINC+a100a6bc56-r0.18/git/src/tbf_dl.cpp:837
#2 0x0002f2574 in gprs_rlcmac_dl_tbf::create_dl_acked_block (this=this@entry=0x5da078, fn=124215, fn@entry=1167128, ts=ts@entry=7 'a', req_mcs_kind=EGPRS, req_mcs_kind@entry=(unknown: 1169532)) at /usr/src/debug/osmo-pcu/0.8.0+gitAUTOINC+a100a6bc56-r0.18/git/src/tbf_dl.cpp:599
#3 0x0003a5ac in sched_select_downlink (bts=0x426d3628, block_nr=55 '?', is_egprs=<synthetic pointer>, req_mcs_kind=(unknown: 1169532), pdch=0x11d87c, fn=1167128, ts=7 'a', trx=optimized out) at /usr/src/debug/osmo-pcu/0.8.0+gitAUTOINC+a100a6bc56-r0.18/git/src/gprs_rlcmac_sched.cpp:343
#4 gprs_rlcmac_rcv_rts_block (bts=0x426d3628, trx=optimized out), ts=optimized out, fn=1167128 , block_nr=9 't'
   at /usr/src/debug/osmo-pcu/0.8.0+gitAUTOINC+a100a6bc56-r0.18/git/src/gprs_rlcmac_sched.cpp:477
#5 0x0001e514 in pcu_rx_rts_req_pdtch (bts=optimized out), trx=optimized out, ts=optimized out, fn=optimized out, block_nr=9 't') at /usr/src/debug/osmo-pcu/0.8.0+gitAUTOINC+a100a6bc56-r0.18/git/src/pcu_l1_if.cpp:384
#6 0x000151f4 in handle_ph_readytosend_ind (fl1h=0x11cc28, rts_ind=0x2ddc28) at /usr/src/debug/osmo-pcu/0.8.0+gitAUTOINC+a100a6bc56-r0.18/git/src/osmo-bts-sysmo/sysmo_l1_if.c:148
#7 11if_handle_l1prim (wq=optimized out), fl1h=0x11cc28, msg=0x2ddc28) at /usr/src/debug/osmo-pcu/0.8.0+gitAUTOINC+a100a6bc56-r0.18/git/src/osmo-bts-sysmo/sysmo_l1_if.c:288
#8 0xb6ed0c94 in ?? () from /usr/lib/libosmocore.so.16

History
#1 - 01/25/2021 12:10 AM - keith
- Subject changed from SEGV in rate_ctr_add() to NULL m_dl_egprs_ctrs passed to rate_ctr_add()

(gdb) up
#1 0x0002f274 in gprs_rlcmac_dl_tbf::create_dl_acked_block (this=this@entry=0x5da078, fn=338684, fn@entry=124215, ts=ts@entry=7 'a', index=0, index@entry=79, index2=-1)
   at /usr/src/debug/osmo-pcu/0.8.0+gitAUTOINC+a100a6bc56-r0.18/git/src/tbf_dl.cpp:837
837 in /usr/src/debug/osmo-pcu/0.8.0+gitAUTOINC+a100a6bc56-r0.18/git/src/tbf_dl.cpp
(gdb) p m_dl_egprs_ctrs
$7 = (rate_ctr_group *) 0x0
(gdb)

#2 - 01/25/2021 04:56 AM - keith

In case it's relevant, on reviewing the crash again:

(gdb) p m_dl_egprs_ctrs
$19 = (rate_ctr_group *) 0x0
(gdb) p m_dl_gprs_ctrs
$20 = (rate_ctr_group *) 0x27ed18
(gdb)

09/18/2022 1/2
I think it should be fixed by this commit, please keith give it a try whenever you have some time:

https://gerrit.osmocom.org/c/osmo-pcu/+/22435 Fix DL EGPRS data blocks being generated occasionally on GPRS TBFs.

I pushed it now to gerrit together with several other fixes of issues I found while looking at osmo-pcu code.

Certainly seems to have fixed the crash.

osmo-pcu.service - Osmocom osmo-pcu
Loaded: loaded (/lib/systemd/system/osmo-pcu.service; enabled; vendor preset: enabled)
Active: active (running) since Mon 2021-01-25 21:12:33 UTC; 7h ago
Main PID: 3571 (osmo-pcu)
CGroup: /system.slice/osmo-pcu.service
└─3571 /usr/bin/osmo-pcu -c /etc/osmocom/osmo-pcu.cfg

Fix merged, closing.