

2.0基站产品化测试 - 错误 #905

UE释放时未释放删除timer导致coredump

2022-08-16 19:44 - b jz

状态:	已关闭	开始日期:	2022-08-16
优先级:	普通	计划完成日期:	
指派给:	王 旭初	% 完成:	0%
类别:		预期时间:	0.00 小时
目标版本:		耗时:	0.00 小时
问题归属:	CU	FPGA板卡类型:	
发现问题版本:	Rel_2.1.10P	CPU类型:	
目标解决问题版本:	Rel_2.1.11P		

描述

```
gdb) bt
#0  gnb::pdcp_timer_msg_comm::send_pdcpc_reordering_timer_expiry_ind (this=this@entry=0x7f140be75df0,
    pdcp_reordering_timer_expiry_ind=pdcp_reordering_timer_expiry_ind@entry=0x7f13b0c76228)
    at /home/bjz/nr_hl_cu/cu/nr_hl_cu/app/build/./src/pdcp_timer_msg_comm.cpp:49
#1  0x00000000074ad16 in gnb::pdcp_rx_rb::on_pdcpc_reordering_timer_expiry (this=0x7f13f0030400)
    at /home/bjz/nr_hl_cu/cu/nr_hl_cu/pdcp/build/./include/pdcp_db.h:2758
#2  0x000000000b75526 in std::function<void (void*)>::operator()(void*) const (__args#0=0x0, this=0x7f13f00389d8)
    at /usr/include/c++/5/functional:2267
#3  ngp::timer_manager::start_timer_thread (this=0x3025350) at /home/bjz/nr_hl_cu/ngp/timer/build/./src/ngp_timer.cpp:131
#4  0x00007f14299c1d4e in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#5  0x00007f14294c56ba in start_thread (arg=0x7f140be76700) at pthread_create.c:333
#6  0x00007f14291fb41d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:109
(gdb) i args
this = 0x7f140be75df0
pdcp_reordering_timer_expiry_ind = 0x7f13b0c76228
(gdb) p 0x7f13b0c76228
$1 = 139722546962984
(gdb) p *0x7f13b0c76228
$2 = -61234960
(gdb) i args
this = 0x7f140be75df0
pdcp_reordering_timer_expiry_ind = 0x7f13b0c76228
(gdb) i locals
msg = <optimized out>
ul_thread = 0x0
(gdb) f 1
#1  0x00000000074ad16 in gnb::pdcp_rx_rb::on_pdcpc_reordering_timer_expiry (this=0x7f13f0030400)
    at /home/bjz/nr_hl_cu/cu/nr_hl_cu/pdcp/build/./include/pdcp_db.h:2758
2758 /home/bjz/nr_hl_cu/cu/nr_hl_cu/pdcp/build/./include/pdcp_db.h: No such file or directory.
(gdb) i args
this = 0x7f13f0030400
(gdb) i locals
pdcp_timer_msg_comm = {<gnb::pdcp_timer_msg_comm_interface> = {
    _vptr.pdcp_timer_msg_comm_interface = 0xbbe9c8 <vtable for gnb::pdcp_timer_msg_comm+16>}, <No data fields>}
(gdb)
```

历史记录

- #1 - 2022-08-16 11:44 - b jz
 - 指派给 被设置为 b jz
- #2 - 2022-08-19 02:53 - b jz
 - 指派给 从 b jz 变更为 席振斌
- #3 - 2022-08-22 03:06 - 席振斌
 - 状态 从 新建 变更为 进行中

#4 - 2022-08-24 07:16 - 席振斌

- 状态从进行中变更为转测试
- 指派给从席振斌变更为王旭初

根据coredump分析，dump的原因为ul_thread为空指针，走读代码发现函数get_specific_ul_thread有可能返回空指针，所以在传递的过程中必须增加保护，在所有用ul_thread传递消息的地方都加了保护

#5 - 2022-09-21 02:17 - 王旭初

- 状态从转测试变更为已解决

测试过程中未出现cu coredump现象，搜索错误打印关键字send_msg_to_ul_thread failed, threadId:，并没有出现该打印，初步评估问题已解决

#6 - 2022-10-13 03:53 - 高峰

- 状态从已解决变更为已关闭