3.0基站产品测试 - 错误 #4460

RLC UM模式下行超流量灌包过程中出现DU COREDUMP

2025-11-19 10:52 - 郭 锁奇

状态:	进行中	**开始日期:**	2025-11-19
优先级:	一般	**计划完成日期:**	
指派给:	韩 伟	**% 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:	DU	**目标解决问题版本:**	Rel_3.1.4
发现问题版本:	Rel_3.1.4		

描述

Rel_3.1.4_Pre1T1版本，RLC UM模式下行超流量灌包过程中出现DU COREDUMP问题。

历史记录

#1 - 2025-11-19 14:02 - 韩 伟

- 状态 从 新建 变更为 进行中

#2 - 2025-11-20 10:58 - 韩 伟

该问题core文件分析，挂死在nrup um模式定时器删除场景。

#3 - 2025-11-20 11:12 - 韩 伟

- 文件 core_stack_print.png 已添加

- 文件 core_stack_print.png 已添加

```
Program terminated with signal SIGSEGV, Segmentation fault.
#0  0x0000000000672180 in cmRmvCbTq (arg=arg@entry=0x7d608c2530) at /home/hw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c:789
789     /home/hw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c: No such file or directory.
[Current thread is 1 (Thread 0x7e0c186b70 (LWP 1259))]
(gdb) bt
#0  0x0000000000672180 in cmRmvCbTq (arg=arg@entry=0x7d608c2530) at /home/hw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c:789
#1  0x0000000000694f64 in cmnHdlCmTmr (tskInfo=0x7d681e9a30) at /home/hw/du_push/ran/nr_hl_du/src/5gnr_cmn//cmn_gcb_hdl.c:468
#2  0x00000000007b5f70 in gnb_du::gnb_du_worker_thread_instance::process_message (this=0x7d5b229b34, p_task=<optimized out>, priority=<optimized out>)
    at /home/hw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/../src/gnb_du_worker_thread.cpp:487
#3  0x000000000075a170 in ngp::thread_pool<gnb_du::gnb_du_worker_thread_instance, ssTskInfo>::thread_worker::run (this=0x1fe7cc50)
    at /home/hw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/../../../../../../../ngp/include/ngp_thread_pool.h:406
#4  0x00000000008da1a4 in thread_start () at /home/hw/du_push/ngp/thread/build/../src/ngp_sys_thread.cpp:338
#5  0x0000007fb97127e4 in start_thread (arg=0x7fe8c2df7f) at pthread_create.c:486
#6  0x0000007fb934470c in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78
```

挂死堆栈信息

#4 - 2025-11-20 11:15 - 韩 伟

- 文件 core_parse.png 已添加

```
(gdb) p *(CmTmrArg *) 0x7d608c2530
$3 = {
  tqCp = 0xe986d8 <cmGCb+339704>,
  tq = 0xe98638 <cmGCb+339544>,
  timers = 0x7d658718bc,
  cb = 538574264372,
  evnt = 185,
  wait = 0,
  tNum = 0 '\000',
  max = 1 '\001'
}
(gdb) p target
No symbol "target" in current context.
(gdb) f 0
#0  0x0000000000672180 in cmRmvCbTq (arg=arg@entry=0x7d608c2530) at /home/hw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c:789
789     /home/hw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c: No such file or directory.
(gdb) p target
$4 = (CmTimer *) 0x7d658718bc
(gdb) p *(CmTimer *) 0x7d658718bc
$5 = {
  tmrEvnt = 125,
  tqExpire = 0,
  cb = 536870912000,
  next = 0x7d5b61a3bc,
  prev = 0x5b98e8bc,
  ent2bUpd = 0 '\000',
  entIdx = 6
}
(gdb) p *(CmTimer *) 0x7d5b61a3bc
$6 = {
  tmrEvnt = 185,
  tqExpire = 1475796,
  cb = 538404037428,
  next = 0x0,
  prev = 0x7d658718bc,
  ent2bUpd = 0 '\000',
  entIdx = 6
}
(gdb) p *(CmTimer *) 0x5b98e8bc
Cannot access memory at address 0x5b98e8bc
```

挂死原因：地址异常

挂死原因为定时器节点内存异常

#5 - 2025-11-20 11:18 - 韩 伟

通过对现有代码梳理，修改前nrup定时器实现机制存在明显问题，在rab释放时，通过发送消息停止定时器，这种机制存在明显的滞后，很容易出现内存释放后已经被其他点申请并使用，导致内存发生变化，滞后的操作再去使用该内存就会挂死。

#6 - 2025-11-20 11:19 - 韩 伟

针对以上不合理机制，已进行代码修改并合入。

文件

core_stack_print.png	33.6 KB	2025-11-20	韩 伟
core_stack_print.png	33.6 KB	2025-11-20	韩 伟
core_parse.png	42.2 KB	2025-11-20	韩 伟