3.0基站产品测试 - 错误 #4348

3.1.3T5版本测试，4UE场景DU COREDUMP问题 timer list内存被踩导致du挂死

2025-10-30 10:01 - 程 鹏

状态:	审视	**开始日期:**	2025-10-30
优先级:	高	**计划完成日期:**	2025-11-30
指派给:	周 立伟	**% 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_3.1.3
发现问题版本:	Rel_3.1.3		

描述

4UE场景有一个DU COREDUMP问题 timer list内存被踩

历史记录

#1 - 2025-10-30 10:02 - 周 立伟

- 指派给 从 周 立伟 变更为 魏 幸幸

#2 - 2025-10-30 10:07 - 周 立伟

- 指派给 从 魏 幸幸 变更为 韩 伟

#3 - 2025-10-30 10:32 - 韩 伟

- 文件 corestack.png 已添加

- 状态 从 新建 变更为 进行中

该问题coredump解析，显示在处理定时器消息过程中异常。

#4 - 2025-10-30 10:34 - 韩 伟

- 文件 corestack.png 已添加

corestack:

```
(gdb) t 1
[Switching to thread 1 (Thread 0x7dee489b70 (LWP 5686))]
#0  0x000000000066e110 in cmPrcTmr (tqCp=0xe7a5c8 <cmGCb+339704>, tq=0xe7a528 <cmGCb+339544>, func=func@entry=0x690d20 <cmnTmrExpiry(unsigned long, cmTimer*)>)
    at /home/zlw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c:238
238     /home/zlw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c: No such file or directory.
(gdb) bt
#0  0x000000000066e110 in cmPrcTmr (tqCp=0xe7a5c8 <cmGCb+339704>, tq=0xe7a528 <cmGCb+339544>, func=func@entry=0x690d20 <cmnTmrExpiry(unsigned long, cmTimer*)>)
    at /home/zlw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c:238
#1  0x0000000000690912a8 in cmnHdlCmTmr (tskInfo=0x7d4c81d030) at /home/zlw/du_push/ran/nr_hl_du/src/5gnr_cmn//cmn_gcb_hdl.c:473
#2  0x00000000007b2930 in gnb_du::gnb_du_worker_thread_instance::process_message (this=0x7d42f29b34, p_task=<optimized out>, priority=<optimized out>)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/../src/gnb_du_worker_thread.cpp:487
#3  0x0000000000755db8 in ngp::thread_pool<gnb_du::gnb_du_worker_thread_instance, ssTskInfo>::thread_worker::run (this=0x234f24f0)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/../../../../../../../ngp/include/ngp_thread_pool.h:406
#4  0x00000000008d4544 in thread_start () at /home/zlw/du_push/ngp/thread/build/../src/ngp_sys_thread.cpp:338
#5  0x0000007f9c2167e4 in start_thread (arg=0x7fd933598f) at pthread_create.c:486
#6  0x0000007f9be4870c in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78
```

#5 - 2025-10-30 10:56 - 韩 伟

core记录数据分析，显示链表：
(gdb) p *(CmTqType *) 0xe7a5a8
$9 = {
first = 0x7d4a5bb164,
tail = 0x7d4b9b4430
}
中存在一个异常节点
(gdb) p *(CmTimer *) 0x7d4a5bb164
$18 = {
tmrEvnt = 125,
tqExpire = 50331649,
cb = 1247523124,

next = 0x0,
prev = 0xffffffff00000000,
ent2bUpd = 0 '\000',
entIdx = 0
}
链表中其他节点均正常，当处理到这个异常节点访问其内存时挂死，通过现有定时器机制分析及异常内存块分析，该定时器内存块应该已经释放掉了，又被其他位置申请，并进行修改，即链表中维护的这个异常节点为残留节点，需要对链表中的节点进行合法性校验，同时也需要自动对链表中异常残留节点进行删除，保障链表节点的有效性。

#6 - 2025-10-30 11:01 - 韩 伟

- 文件 异常节点内存块快照.png 已添加

- 文件 正常节点内存块快照.png 已添加

异常节点内存块快照

```
(gdb) x/100xw 0x7d4a5bb100
0x7d4a5bb100:   0x00630637      0x4e040003      0x202dec5e      0xdbeb8b6f
0x7d4a5bb110:   0x483cff10      0x0000007d      0xe5e5e5e5      0xe5e5e5e5
0x7d4a5bb120:   0x00000000      0x00000000      0x00000000      0x00000000
0x7d4a5bb130:   0x14400a00      0x00030000      0x00000000      0x00000000
0x7d4a5bb140:   0x00000000      0x00000000      0x4ebbff30      0x0000007d
0x7d4a5bb150:   0x4a5bb1b0      0x0000007d      0x4a5bb1b1      0x0000007d
0x7d4a5bb160:   0x4a5bb168      0x0000007d      0x03000001      0x4a5bb134
0x7d4a5bb170:   0x00000000      0x00000000      0x00000000      0x00000000
0x7d4a5bb180:   0xffffffff      0x00000000      0x00000000      0x00000000
0x7d4a5bb190:   0x00000000      0x00000000      0x00000000      0x00000000
0x7d4a5bb1a0:   0x4a5bb1b0      0x0000007d      0x4a5bb210      0x0000007d
0x7d4a5bb1b0:   0x81400bff      0x00050000      0x00020029      0x006f0028
0x7d4a5bb1c0:   0xf1000009      0x00000010      0x5f001000      0x42000300
0x7d4a5bb1d0:   0x003200a6      0x00000607      0xc23f0000      0x80008000
0x7d4a5bb1e0:   0x39383736      0x33323130      0x37363534      0x37363938
0x7d4a5bb1f0:   0x31303938      0x35343332      0x39383736      0x33323130
0x7d4a5bb200:   0x00750b34      0x4e040003      0x202dec5e      0x559050b5
0x7d4a5bb210:   0x4b6d9d10      0x0000007d      0xe5e5e5e5      0xe5e5e5e5
0x7d4a5bb220:   0x00000000      0x00000000      0x00000000      0x00000000
0x7d4a5bb230:   0x906d0002      0x0000058c      0x49d0ef30      0x0000007d
0x7d4a5bb240:   0x4b6d9d30      0x0000007d      0x00000000      0x00000000
0x7d4a5bb250:   0x61f48047      0x0000007d      0x00000584      0x00000000
0x7d4a5bb260:   0x0000044d      0x00000000      0x48ee5030      0x0000007d
0x7d4a5bb270:   0xfc3bcd48      0x00000000      0x0003cd48      0x00000000
0x7d4a5bb280:   0x00000118      0x00000000      0x00000000      0x00000000
(gdb) x/300xw 0x7d4a5bb100
```

正常节点内存块快照

#7 - 2025-10-30 11:02 - 韩 伟

- 文件 正常节点内存块快照.png 已添加

```
(gdb) x/100xw 0x7d4b9b4400
0x7d4b9b4400:   0x36353433      0x30393837      0x00000000      0x00000000
0x7d4b9b4410:   0x43e13d10      0x0000007d      0xe5e5e5e5      0xe5e5e5e5
0x7d4b9b4420:   0xdeadbeaf      0x00000000      0x00000000      0x00000000
0x7d4b9b4430:   0x00000042      0x032e5950      0x8a3e0030      0x0000007d
0x7d4b9b4440:   0x00000000      0x00000000      0x4304cf30      0x0000007d
0x7d4b9b4450:   0x00080000      0x00000000      0x0002a49f      0x00000000
0x7d4b9b4460:   0x00000000      0x00000000      0x00000000      0x00000000
0x7d4b9b4470:   0x00000000      0x00000000      0x00000000      0x00000000
0x7d4b9b4480:   0x00000000      0x00000000      0x00010000      0x00000000
0x7d4b9b4490:   0x0000004b      0x917e1048      0x0000007d      0x000042f7
0x7d4b9b44a0:   0x4b9b44b0      0x0000007d      0x4b9b4510      0x0000007d
0x7d4b9b44b0:   0x38373635      0x32313039      0x36353433      0x30393837
0x7d4b9b44c0:   0x34333231      0x38373635      0x32313039      0x36353433
0x7d4b9b44d0:   0x30393837      0x34333231      0x38373635      0x32313039
0x7d4b9b44e0:   0x36353433      0x30393837      0x34333231      0x38373635
0x7d4b9b44f0:   0x32313039      0x36353433      0x30393837      0x34333231
0x7d4b9b4500:   0x00800235      0x4e040000      0x402dec5e      0x03eaa758
0x7d4b9b4510:   0x48c6ab10      0x0000007d      0xe5e5e5e5      0xe5e5e5e5
0x7d4b9b4520:   0x00000000      0x00000000      0x00000000      0x00000000
0x7d4b9b4530:   0x625fb047      0x0000007d      0x625fb03a      0x0000007d
0x7d4b9b4540:   0x625fb030      0x0000007d      0x00000000      0x00000000
0x7d4b9b4550:   0x00000584      0x0000007d      0x056607d0      0x00000453
0x7d4b9b4560:   0x00000113      0x00000566      0x00000000      0xdf5857c9
0x7d4b9b4570:   0x00000000      0x000057c9      0xbf4a0da9      0x0000009a
0x7d4b9b4580:   0x000002b6      0x00000000      0x00000000      0x00000000
```

正常节点内存块快照

#8 - 2025-10-30 11:13 - 韩 伟

目前针对此种情况，已对定时器链表节点合法性进行校验，并对非法节点进行清理进行了修改，以保障链表可以正常处理下去。修改版本自测通过，无害验证已完成。

#9 - 2025-11-04 20:08 - 韩 伟

- 状态 从 进行中 变更为 审视

- 指派给 从 韩 伟 变更为 周 立伟

版本已合入T8。

文件

corestack.png	37.6 KB	2025-10-30	韩 伟
corestack.png	37.6 KB	2025-10-30	韩 伟
异常节点内存块快照.png	33.7 KB	2025-10-30	韩 伟
正常节点内存块快照.png	32.4 KB	2025-10-30	韩 伟
正常节点内存块快照.png	32.4 KB	2025-10-30	韩 伟