

B5G_UE - 错误 #3335

threadL3在mac的OM广播打桩下崩溃在malloc

2025-05-14 17:21 - 李 玮璇

状态:	已解决	开始日期:	2025-05-14
优先级:	紧急	计划完成日期:	
指派给:	李 玮璇	% 完成:	100%
类别:		预期时间:	16.00 小时
目标版本:		耗时:	0.00 小时
描述			
如题，mac打桩OM广播接收流程，会导致threadL3在不同环境崩溃在不同地方； 有个崩溃如下： Thread 5 "threadL3" received signal SIGSEGV, Segmentation fault. [Switching to Thread 0x7fff4a61700 (LWP 126117)] _int_malloc (av=av@entry=0x7ffec000020, bytes=bytes@entry=654) at malloc.c:3789 3789 malloc.c: No such file or directory. (gdb) bt #0 _int_malloc (av=av@entry=0x7ffec000020, bytes=bytes@entry=654) at malloc.c:3789 #1 0x00007ffff65290d1 in __libc_calloc (n=<optimized out>, elem_size=<optimized out>) at malloc.c:3446 #2 0x00005555565f2ccf in wnCreateRb (rrcCb=0x7ffec003ee0, rbType=WN_RB_TYPE_SRB_E, rbId=1 '\001') at src/I3/rrc/csrc/wn5gNrUePsRrcSetUpRqst.c:529 #3 0x00005555561a9563 in wnRrcNcDevAddHandler (ssCpCb=0x7ffec003ea0, trans=0x7ffec004f70, msg=0x0) at src/I3/rrc/csrc/wn5gNrUePsRrcNcHndlr.c:84 #4 0x00005555563bbe45 in procTransEvent (ssCpCb=0x7ffec003ea0, trans=0x7ffec004f70, msg=0x0) at src/I3/rrc/csrc/wn5gNrUePsRrcTrans.c:240 #5 0x00005555563c2fc3 in procTrans (ssCpCb=0x7ffec003ea0, msg=0x0, event=WN_TRANS_RRC_NC_DEV_ADD_E) at src/I3/rrc/csrc/wn5gNrUePsRrcTrans.c:285 #6 0x000055555622a2d4 in wnRrcNcDevFindProcess (ssCb=0x55555bd21480, devId=4 '\004') at src/I3/rrc/csrc/wn5gNrUePsRrcNcHndlr.c:717 #7 0x0000555556243acf in wnSsRrcPollNcRxCfgMsg (ssCb=0x55555bd21480, mpi=0x22016a7c00) at src/I3/rrc/csrc/wn5gNrUePsRrcNcHndlr.c:824 #8 0x0000555556ab00ee in threadL3 (ueCb=0x55555ba688e0) at src/I3/rrc/csrc/yzL3Mani.c:371 #9 0x000055555a2d9e5a in eal_thread_loop () #10 0x00007ffff68876db in start_thread (arg=0x7fff4a61700) at pthread_create.c:463 #11 0x00007ffff65b061f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95产生的可能原因			

历史记录

#1 - 2025-05-14 17:40 - 李 玮璇

- 状态从新建 变更为 进行中

原因：1、wnVoid>(*transFsm[MAX_TRANS_STATES][MAX_TRANS_EVENTS])(); 宏定义不够导致越界踩内存
2、double free free(stub->securityConfig);
修改：421053e7a69771e75d205eb716cd27089890306f，已合入 'Bug_fixed_ps0506'

#2 - 2025-05-14 17:40 - 李 玮璇

- 状态从进行中 变更为 已解决

#3 - 2025-05-14 17:49 - 李 玮璇

- % 完成从0 变更为100

- 预期时间被设置为16.00 小时