

FC子项目 - 错误 #275

ueradio_capability_for_paging_of_nr cause coredump

2020-12-08 21:05 - b jz

状态:	已关闭	开始日期:	2020-12-08
优先级:	普通	计划完成日期:	
指派给:	b jz	% 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:			

描述

```
(gdb) bt
#0  __GI___libc_free (mem=0x6015e00) at malloc.c:2951
#1  0x00000000008fccf8 in ngap::initial_context_setup_request::~initial_context_setup_request (this=0x7fb8a0021a80,
    __in_chrg=<optimized out>)
    at /home/bjz/nr_hl_cu/cu/nr_hl_cu/ue_conn_mgr/build/../../common/include/../../ngap_codec/include/ngap_msg_types.h:3187
#2  gnb::conn_mgmt::process_ng_intial_context_setup_req (this=this@entry=0x7fb8e2cd86f7, asn_msg=...)
    at /home/bjz/nr_hl_cu/cu/nr_hl_cu/ue_conn_mgr/build/./src/ue_conn_mgr_ng_msg.cpp:207
#3  0x00000000008ff220 in gnb::conn_mgmt::process_ng_msg (this=this@entry=0x7fb8e2cd86f7, cntrl_ref_id=...,
    ng_msg_type=<optimized out>, asn_msg=...)
    at /home/bjz/nr_hl_cu/cu/nr_hl_cu/ue_conn_mgr/build/./src/ue_conn_mgr_ng_msg.cpp:521
#4  0x00000000008cfd14 in gnb::ue_conn_mgr_msg_hdlr::process_sctp_user_msg_rx_ind (this=<optimized out>,
    sctp_user_msg_rx_ind=0x7fb8a8030bf0) at /home/bjz/nr_hl_cu/cu/nr_hl_cu/ue_conn_mgr/build/./src/ue_conn_mgr_msg_hdlr.cpp:8
4
#5  0x000000000083349e in gnb::ue_cntrl_thread::process_message (this=0x2030d40, message=0x7fb8a8010bb0)
    at /home/bjz/nr_hl_cu/cu/nr_hl_cu/app/build/./src/ue_cntrl_thread.cpp:69
#6  0x00000000007836a4 in ngp::comm_thread::run (this=0x2030d40)
    at /home/bjz/nr_hl_cu/cu/nr_hl_cu/app/build/../../ngp/include/ngp_comm_thread.h:220
#7  0x0000000000aac687 in ngp::thread_entry_function (param=0x2030d40)
    at /home/bjz/nr_hl_cu/ngp/thread/build/./src/ngp_sys_thread.cpp:110
#8  ngp::thread_start (param=0x2030d40) at /home/bjz/nr_hl_cu/ngp/thread/build/./src/ngp_sys_thread.cpp:123
#9  0x00007fb8ff86e6ba in start_thread (arg=0x7fb8e2cd9700) at pthread_create.c:333
#10 0x00007fb8ff5a441d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:109
```

历史记录

- #1 - 2020-12-08 21:05 - b jz
- 状态 从 新建 变更为 进行中
- ASN解码赋值导致踩内存。先临时修改提交，用于发布版本。稍后彻底修改。先不关闭MR。
- #2 - 2020-12-08 21:05 - b jz
- 关联GITLAB http://192.168.1.104/YZRT/5gnr/nr_hl_cu/issues/15
- #3 - 2020-12-14 17:53 - b jz
- 状态 从 进行中 变更为 已解决
- 修改修改BITSTRING LONG 的decode和存储方式，匹配了encode的方式，解决了存储越界的问题。
- #5 - 2020-12-14 18:05 - b jz
- 状态 从 已解决 变更为 已关闭