

B5G_UE - 错误 #2599

FAPI 联调 SIB1打桩coredump

2024-12-24 10:53 - b jz

状态:	已解决	开始日期:	2024-12-24
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
描述			
播雨反馈SIB1打桩后 coredump			
<pre>(gdb) bt #0 wnSendInfoToNas (sibOneInfo=0x7dc4001e40) at src/l3//csrc/wn5gNrUePsIdleHndlr.c:350 #1 0x000000000109720c in wnSibAcquire (Cb=0x1f4ac2d0, buffRcvd=0x7dc4001e10) at src/l3//csrc/wn5gNrUePsIdleHndlr.c:297 #2 0x00000000010851bc in wnSiAcq (Cb=0x1f4ac2d0, mbufPool=0x17f20d080) at src/l3//csrc/wn5gNrUePsIdleHndlr.c:136 #3 0x0000000000b9bcd8 in wnPlmnSearch (cpCb=0x1f49b830, msg=0x17f20d080) at src/l3//csrc/wn5gNrUePsEvntsHndlr.c:66 #4 0x000000000034ed28c in wnPlmnSearchHandler (cpCbRcvd=0x1f49b830) at src/l3/nas/csrc/wn5gNrUePsNasMmState.c:83 #5 0x000000000034fd1ec in wnCellSelHandler (cpCbRcvd=0x1f49b830, data=0x0) at src/l3/nas/csrc/wn5gNrUePsNasMmState.c:163 #6 0x000000000012e7048 in threadL3 (ueCb=0x1f49b1c0) at src/l3//csrc/yzL3Mani.c:185 #7 0x00000000004155748 in eal_thread_loop () #8 0x000000007f89d7a7e4 in start_thread (arg=0x7fdfe865ef) at pthread_create.c:486 #9 0x000000007f89c0070c in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78 (gdb) i args sibOneInfo = 0x7dc4001e40 (gdb) p *sibOneInfo \$1 = {sibOne = 0x0, buff = 0x175446600 <error: Cannot access memory at address 0x175446600>, Cb = 0x1f4ac2d0, selFrqBand = 0 '\000', priorityOfSelFreqBand = 0, selAddSptrmEm = 0 '\000', frqBandList = 0x49cdc80 <frqBandList.31390>}</pre>			

历史记录

#1 - 2024-12-24 10:55 - b jz

和播雨联调发现，如果SIB1消息出错导致解码错误后，代码为做保护继续往后跑。导致取空指针值。从而coredum0p

#2 - 2024-12-24 11:07 - b jz

<http://192.168.1.104/YZRT/b5gue/b5gueps/issues/62>

#3 - 2024-12-24 11:07 - b jz

提交代码，待测试。

#4 - 2024-12-24 15:11 - b jz

包 敬重 写到：

和播雨联调发现，如果SIB1消息出错导致解码错误后，代码为做保护继续往后跑。导致取空指针值。从而coredum0p

未做

#5 - 2025-01-03 17:14 - b jz

测试完成

#6 - 2025-01-11 12:06 - 李常

- 指派给 被设置为 b jz

#7 - 2025-01-15 10:37 - b jz

- 描述 已更新。

- 状态 从 新建 变更为 转测试

#8 - 2025-01-15 10:37 - b jz
- 状态从 转测试 变更为 已解决

#9 - 2025-02-10 12:22 - 李 常
未再发生，close it.