3.0基站产品测试 - 错误 #5204

-fsanitize=address 内存检查

2026-04-24 16:41 - 李 宇哲

状态:	新建	**开始日期:**	2026-04-24
优先级:	一般	**计划完成日期:**	
指派给:	李 宇哲	**% 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_3.2.1
发现问题版本:	Rel_3.2.1		

描述

-fsanitize=address 是 GCC 和 Clang 编译器的一个选项，用于启用 AddressSanitizer（ASan），这是一个内存错误检测工具

历史记录

#1 - 2026-04-24 16:43 - 李 宇哲

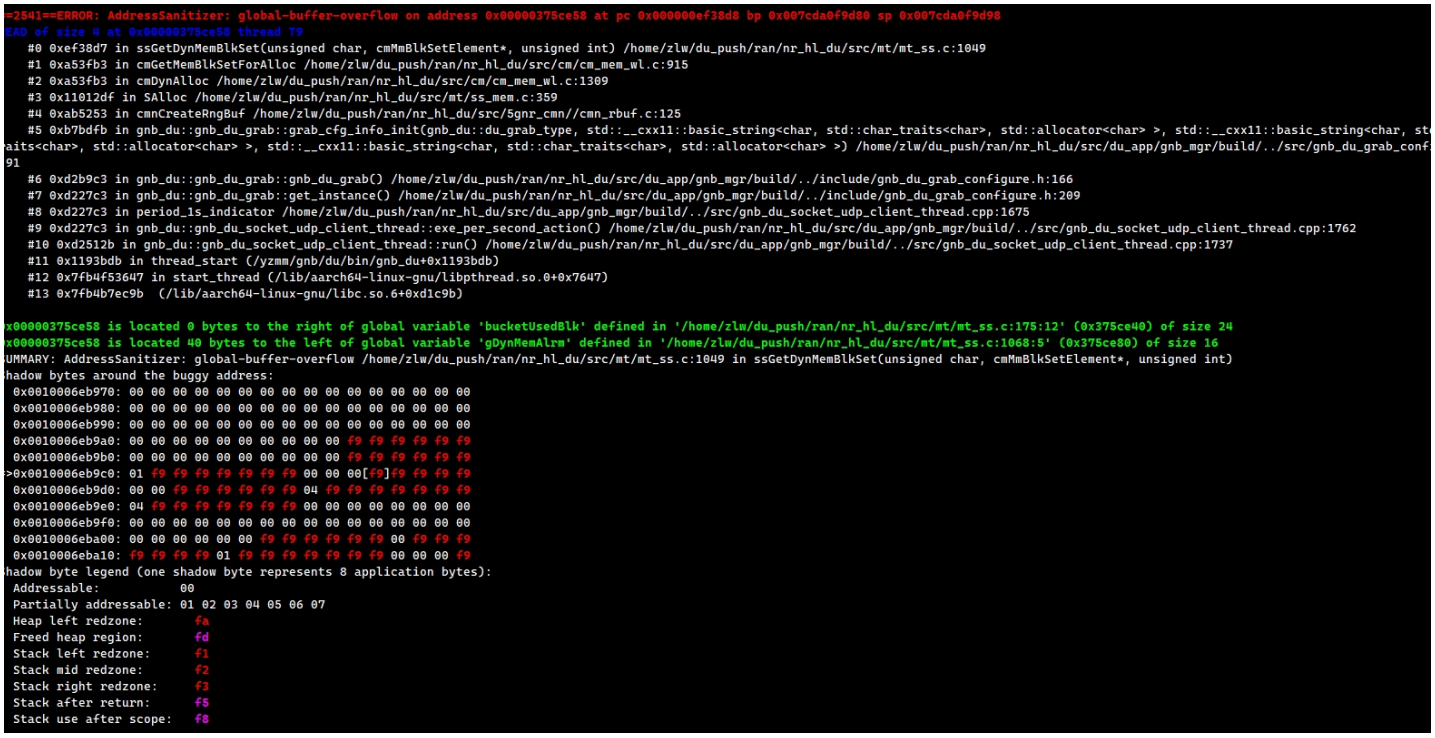
- 文件 20260424-164236.jpg 已添加

- 文件 20260424-164248.jpg 已添加

- 文件 屏幕截图 2026-04-24 161603.png 已添加

目前DU发现两个问题，ap_driver发现一个问题

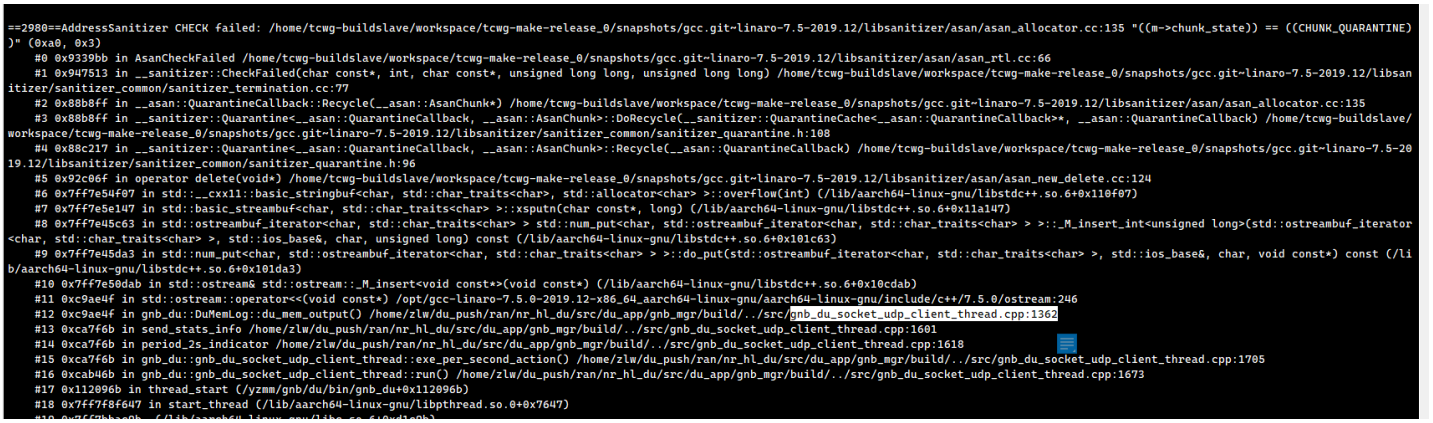
```
=================================================================
==1035==ERROR: AddressSanitizer: global-buffer-overflow on address 0x000003759f98 at pc 0x000000ef2374 bp 0x007fd0c4b430 sp 0x007fd0c4b448
READ of size 4 at 0x000003759f98 thread T0 (gnb_du)
    #0 0xef2373 in SAllocateWlsDynMem /home/zlw/du_push/ran/nr_hl_du/src/mt/mt_ss.c:1176
    #1 0xef2373 in ssdInitMem /home/zlw/du_push/ran/nr_hl_du/src/mt/mt_ss.c:1257
    #2 0x10fbf3b in SInit /home/zlw/du_push/ran/nr_hl_du/src/mt/ss_gen.c:279
    #3 0x7aeef7 in main /home/zlw/du_push/ran/nr_hl_du/src/mt/mt_ss.c:735
    #4 0x7f93b43dd7 in __libc_start_main (/lib/aarch64-linux-gnu/libc.so.6+0x20dd7)
    #5 0x8ee2b7  (/yzmm/gnb/du/bin/gnb_du+0x8ee2b7)

0x000003759f98 is located 0 bytes to the right of global variable 'mtDynMemSz' defined in '/home/zlw/du_push/ran/nr_hl_du/src/mt/mt_ss.c:623:20' (0x3759f20) of size 120
0x000003759f98 is located 40 bytes to the left of global variable 'TtiCount' defined in '/home/zlw/du_push/ran/nr_hl_du/src/mt/mt_ss.c:4342:7' (0x3759fc0) of size 8
SUMMARY: AddressSanitizer: global-buffer-overflow /home/zlw/du_push/ran/nr_hl_du/src/mt/mt_ss.c:1176 in SAllocateWlsDynMem
Shadow bytes around the buggy address:
  0x0010006eb3a0: 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9 f9 f9
  0x0010006eb3b0: 00 00 00 00 00 f9 f9 f9 f9 f9 f9 f9 01 f9 f9 f9
  0x0010006eb3c0: f9 f9 f9 f9 00 00 00 f9 f9 f9 f9 f9 00 00 f9 f9
  0x0010006eb3d0: f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9
  0x0010006eb3e0: f9 f9 f9 f9 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0010006eb3f0: 00 00 00[f9]f9 f9 f9 f9 00 f9 f9 f9 f9 f9 f9 f9
  0x0010006eb400: 01 f9 f9 f9 f9 f9 f9 f9 00 00 00 f9 f9 f9 f9 f9
  0x0010006eb410: 00 00 00 f9 f9 f9 f9 f9 00 00 00 f9 f9 f9 f9 f9
  0x0010006eb420: 00 00 00 f9 f9 f9 f9 f9 00 00 00 f9 f9 f9 f9 f9
  0x0010006eb430: 00 00 00 00 f9 f9 f9 f9 00 f9 f9 f9 f9 f9 f9 f9
  0x0010006eb440: 00 f9 f9 f9 f9 f9 f9 f9 00 00 00 00 01 f9 f9 f9
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
```



屏幕截图 2026-04-24 161603.png

#2 - 2026-04-24 16:43 - 李 宇哲

- 文件 屏幕截图 2026-04-24 160235.png 已添加



#3 - 2026-04-24 16:44 - 李 宇哲

- 文件 已删除 (屏幕截图 2026-04-24 161603.png)

文件

20260424-164236.jpg	389 KB	2026-04-24	李 宇哲
20260424-164248.jpg	659 KB	2026-04-24	李 宇哲
屏幕截图 2026-04-24 160235.png	111 KB	2026-04-24	李 宇哲