New issue

Jump to bottom

SEGV found in server_example1 #8

Open **Rrooach** opened this issue on Oct 10, 2019 · 0 comments

Rrooach commented on Oct 10, 2019

Hello, I found a **SEGV** in libiec_iccp_mod/examples/server_example1/server_example1.c

Below are steps followed to reproduce crash
Download latest source code from: /fcovatti/libiec_iccp_mod/, compiled with clang and ASAN `export CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address"` before make

Row data
crash.zip

ASAN Output

```
ASAN:DEADLYSIGNAL
=================================================================
==8829==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000005da850 bp 0x000000000002 sp 0x7fd097afbd20 T4)          ==8829==The signal is caused by a READ
memory access.                                                                                  ==8829==Hint: address points to the zero page.
    #0 0x5da84f in AcseConnection_parseMessage /root/libiec_iccp_mod/src/mms/iso_acse/acse.c:341
    #1 0x5980a0 in handleTcpConnection /root/libiec_iccp_mod/src/mms/iso_server/iso_connection.c:145
    #2 0x53a371 in destroyAutomaticThread /root/libiec_iccp_mod/src/hal/thread/linux/thread_linux.c:87
    #3 0x7fd09ca906b9 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76b9)
    #4 0x7fd09be9b41c in clone /build/glibc-LK5gWL/glibc-2.23/misc/../sysdeps/unix/sysv/linux/x86_64/clone.S:109

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /root/libiec_iccp_mod/src/mms/iso_acse/acse.c:341 in AcseConnection_parseMessage
Thread T4 created by T1 here:
    #0 0x4327dd in __interceptor_pthread_create (/root/temp/iec/libiec_iccp_mod/examples/server_example1/server_example1+0x4327dd)
    #1 0x53a5e2 in Thread_start /root/libiec_iccp_mod/src/hal/thread/linux/thread_linux.c:98

Thread T1 created by T0 here:
    #0 0x4327dd in __interceptor_pthread_create (/root/temp/iec/libiec_iccp_mod/examples/server_example1/server_example1+0x4327dd)
    #1 0x53a5bd in Thread_start /root/libiec_iccp_mod/src/hal/thread/linux/thread_linux.c:102

==8829==ABORTING
```

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant