


New issue

[Jump to bottom](#)

SEGV in function lec104_Deal_FirmUpdate #5

 Closed luckyzfl opened this issue on Mar 17, 2019 · 0 comments

luckyzfl commented on Mar 17, 2019 • edited

Hello, I built protocol IEC104 in my ubuntu16.04 machine with AddressSanitizer(export CFLAGS="-g -fsanitize=address" CXXFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" before make).

And I use [preeny desock](#) tool to build channels socket communication to the console.

But when I use the following data (here in hexadecimal format for easy understanding but must be inputted as binary format file) as the input to the server socket 10000, there will be a SEGV during the running.

```
68:e0:40:00:00:83:80:68 10:00:00:00:00:00:00 00:00:00:00:00:00:00 00:00:00:00:00:00:00 00:00:00:00:00:00:00 80:00:08
```

The way I built iec104_monitor is as you sad [here](#), just cut the main function to the bottom in ./test/main.c and change the route of source files in ./test/Makefile .

The command line is as follows:

```
LD_PRELOAD="/usr/lib/x86_64-linux-gnu/libasan.so.2:/root/preeny/x86_64-linux-gnu/desock.so" ./iec104_monitor -m server -n 1 < ./test_input
```

where

/usr/lib/x86_64-linux-gnu/libasan.so.2 is the lib of asan,

/root/preeny/x86_64-linux-gnu/desock.so is the lib of preeny desock

./test_input is the binary format file which contains the test input as mentioned above in hexadecimal format for easy understanding.

The run time error information is:

```
Register "Linux" IEC104 Success, < HuiXing 2014-2015 > ...
mode : (0), port: (0), ip: (), station num: (1)
Iec104 Server Mode
Iec104 Socket Ok(10000) !
Iec104 Bind Ok(10000) !
Iec104 Listen Ok(10000)
Accept ok!
Server start get connect from 0 : 0x2328
#####received
[DumpHEX]Length:43
68:e0:40:00:00:83:80:68 10:00:00:00:00:00:00
00:00:00:00:00:00:00 00:00:00:00:00:00:00
00:00:00:00:00:00:83 80:00:08
-Iex104_Receive-,Frame Type I
Receive Package I(32,16768), Send(0,0)
+++Asdu Type Firmware Update...
-Iec104_Deal_FirmUpdate-,data finish:0,Len:208,Total Len:0
ASAN:SIGSEGV
=====
==26583==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x000000000000 bp 0x000000000000 sp 0x7fb0d0cfe4e8 T1)
==26583==Hint: pc points to the zero page.

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ??:0 ??
Thread T1 created by T0 here:
#0 0x7fb0d4376253 in pthread_create (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x36253)
#1 0x4020a9 in main /root/feilong/libiec104_fuzz/asan-mode/IEC10X/main.c:299

==26583==ABORTING
```

I use gdb to debug it and the information is as following:

```
Thread 2 "iec104_monitor" received signal SIGSEGV, Segmentation fault.
[Switching to Thread 0x7ffff37ff700 (LWP 19690)]
0x0000000000000000 in ?? ()
(gdb) backtrace
#0 0x0000000000000000 in ?? ()
#1 0x000000000040898d in Iec104_Deal_FirmUpdate (asdu=asdu@entry=0x7ffff37fe886, Len=Len@entry=226 '\342') at ../IEC10X/Iec104.c:1129
#2 0x000000000040a631 in Iec104_Deal_I (Iec104Data=Iec104Data@entry=0x7ffff37fe880, len=Len@entry=226) at ../IEC10X/Iec104.c:1208
#3 0x000000000040adac in Iex104_Receive (buf=buf@entry=0x7ffff37fe880 "h\340@", len=len@entry=43) at ../IEC10X/Iec104.c:1305
#4 0x000000000040fe67 in Iec104_main (arg=coptimized out) at main.c:138
#5 0x00007ffff6a306ba in start_thread (arg=0x7ffff37ff700) at pthread_create.c:333
#6 0x00007ffff676641d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:109
(gdb)
#0 0x0000000000000000 in ?? ()
#1 0x000000000040898d in Iec104_Deal_FirmUpdate (asdu=asdu@entry=0x7ffff37fe886, Len=Len@entry=226 '\342') at ../IEC10X/Iec104.c:1129
#2 0x000000000040a631 in Iec104_Deal_I (Iec104Data=Iec104Data@entry=0x7ffff37fe880, len=Len@entry=226) at ../IEC10X/Iec104.c:1208
#3 0x000000000040adac in Iex104_Receive (buf=buf@entry=0x7ffff37fe880 "h\340@", len=len@entry=43) at ../IEC10X/Iec104.c:1305
#4 0x000000000040fe67 in Iec104_main (arg=coptimized out) at main.c:138
#5 0x00007ffff6a306ba in start_thread (arg=0x7ffff37ff700) at pthread_create.c:333
#6 0x00007ffff676641d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:109
(gdb)
```

 This was referenced on Mar 17, 2019

SEGV in function lec104_Deal_FirmUpdate which is different from issue#5 #6

 Closed

New SEGV in function lec104_Deal_FirmUpdate which is different from issue#5 and issue#6 #7

 Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

