New issue

Jump to bottom

Heap-buffer-overflow found in client_example1.c #5

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

Rrooach commented on Oct 10, 2019

Hello, I found a potential heap-buffer-overflow in /libiec_iccp_mod/examples/iec61850_client_example1/client_example1.c, seems in some case when the packet can not be accept, the program throw cause heap-buffer-overflow.

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

ASAN Output:

```
=================================================================
==7794==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6280000040ff at pc 0x00000048e8df bp 0x7ffffed8b350 sp 0x7ffffed8ab00    WRITE of size 13 at 0x6280000040ff
thread T0                                                                                           � ��      #0 0x48e8de in read
(/root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1+0x48e8de)
    #1 0x61d236 in read /usr/include/x86_64-linux-gnu/bits/unistd.h:44
    #2 0x61d236 in Socket_read /root/libiec_iccp_mod/src/hal/socket/linux/socket_linux.c:309
    #3 0x681f3c in ByteStream_readOctets /root/libiec_iccp_mod/src/common/byte_stream.c:108
    #4 0x62ccdd in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:577
    #5 0x62ccdd in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #6 0x62f02f in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:590
    #7 0x62f02f in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #8 0x62f02f in CotpConnection_parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:650
    #9 0x5bfae5 in IsoClientConnection_associate /root/libiec_iccp_mod/src/mms/iso_client/impl/iso_client_connection.c:328
    #10 0x5b1805 in MmsConnection_connect /root/libiec_iccp_mod/src/mms/iso_mms/client/mms_client_connection.c:887
    #11 0x53c6ba in IedConnection_connect /root/libiec_iccp_mod/src/iedclient/impl/ied_connection.c:472
    #12 0x511c51 in main /root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1.c:49:5
    #13 0x7f0fafea182f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/../csu/libc-start.c:291
    #14 0x41a738 in _start (/root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1+0x41a738)

0x6280000040ff is located 1 bytes to the left of 16100-byte region [0x628000004100,0x628000007fe4)                                    ==7794==AddressSanitizer CHECK failed:
/build/llvm-toolchain-5.0-DI81tt/llvm-toolchain-5.0-5.0/projects/compiler-rt/lib/asan/asan_descriptions.cc:178 "((res.trace)) != (0)" (0x0, 0x0)
    #0 0x4e567f in __asan::AsanCheckFailed(char const*, int, char const*, unsigned long long, unsigned long long)
(/root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1+0x4e567f)
    #1 0x501755 in __sanitizer::CheckFailed(char const*, int, char const*, unsigned long long, unsigned long long)
(/root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1+0x501755)
    #2 0x427b74 in __asan::HeapAddressDescription::Print() const (/root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1+0x427b74)
    #3 0x42b376 in __asan::ErrorGeneric::Print() (/root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1+0x42b376)    #4 0x4e0f2b in
__asan::ReportGenericError(unsigned long, unsigned long, unsigned long, unsigned long, bool, unsigned long, unsigned int, bool) [clone .part.11]
(/root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1+0x4e0f2b)
    #5 0x48e8fc in read (/root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1+0x48e8fc)
    #6 0x61d236 in read /usr/include/x86_64-linux-gnu/bits/unistd.h:44
    #7 0x61d236 in Socket_read /root/libiec_iccp_mod/src/hal/socket/linux/socket_linux.c:309
    #8 0x681f3c in ByteStream_readOctets /root/libiec_iccp_mod/src/common/byte_stream.c:108
    #9 0x62ccdd in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:577
    #10 0x62ccdd in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #11 0x62f02f in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:590
    #12 0x62f02f in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #13 0x62f02f in CotpConnection_parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:650
    #14 0x5bfae5 in IsoClientConnection_associate /root/libiec_iccp_mod/src/mms/iso_client/impl/iso_client_connection.c:328
    #15 0x5b1805 in MmsConnection_connect /root/libiec_iccp_mod/src/mms/iso_mms/client/mms_client_connection.c:887
    #16 0x53c6ba in IedConnection_connect /root/libiec_iccp_mod/src/iedclient/impl/ied_connection.c:472
    #17 0x511c51 in main /root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1.c:49:5
    #18 0x7f0fafea182f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/../csu/libc-start.c:291
    #19 0x41a738 in _start (/root/temp/iec/libiec_iccp_mod/examples/iec61850_client_example1/client_example1+0x41a738)
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant