Heap-buffer-overflow found at mms_client_example1.c #6

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/mms_client_example1/mms_client_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:
Uploading crash.zip…

ASAN Output:

```
==19279==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6280000040fd at pc 0x00000048e36f bp 0x7f
fe7f010010 sp 0x7ffe7f00f7c0   WRITE of size 223 at 0x6280000040fd thread T0 #0 0x48e36e in read
(/root/temp/iec/libiec_iccp_mod/examples/mms_client_example1/mms_client_example1+0x48e36e)            #1 0x57b266 in read /usr/include/x86_64-linux-gnu/bits/unistd.h:44
    #2 0x57b266 in Socket_read /root/libiec_iccp_mod/src/hal/socket/linux/socket_linux.c:309
    #3 0x5e98cc in ByteStream_readOctets /root/libiec_iccp_mod/src/common/byte_stream.c:108
    #4 0x5a128d in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:577
    #5 0x5a128d in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #6 0x5a13df in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:590
    #7 0x5a13df in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #8 0x5a13df in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:590
    #9 0x5a13df in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #10 0x5a35df in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:590
    #11 0x5a35df in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #12 0x5a35df in CotpConnection_parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:650
    #13 0x522dac in IsoClientConnection_associate /root/libiec_iccp_mod/src/mms/iso_client/impl/iso_client_connection.c:382
    #14 0x514885 in MmsConnection_connect /root/libiec_iccp_mod/src/mms/iso_mms/client/mms_client_connection.c:887
    #15 0x5113e4 in main /root/temp/iec/libiec_iccp_mod/examples/mms_client_example1/mms_client_example1.c:38:6
    #16 0x7f9d34dc982f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/../csu/libc-start.c:291
    #17 0x41a1c8 in _start (/root/temp/iec/libiec_iccp_mod/examples/mms_client_example1/mms_client_example1+0x41a1c8)

0x6280000040fd is located 3 bytes to the left of 16100-byte region [0x628000004100,0x628000007fe4)                          ==19279==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 0x4e510f in __asan::AsanCheckFailed(char const*, int, char const*, unsigned long long, unsigned long long)
(/root/temp/iec/libiec_iccp_mod/examples/mms_client_example1/mms_client_example1+0x4e510f)
    #1 0x5011e5 in __sanitizer::CheckFailed(char const*, int, char const*, unsigned long long, unsigned long long)
(/root/temp/iec/libiec_iccp_mod/examples/mms_client_example1/mms_client_example1+0x5011e5)
    #2 0x427604 in __asan::HeapAddressDescription::Print() const (/root/temp/iec/libiec_iccp_mod/examples/mms_client_example1/mms_client_example1+0x427604)
    #3 0x42ae06 in __asan::ErrorGeneric::Print() (/root/temp/iec/libiec_iccp_mod/examples/mms_client_example1/mms_client_example1+0x42ae06)     #4 0x4e09bb 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/mms_client_example1/mms_client_example1+0x4e09bb)
    #5 0x48e38c in read (/root/temp/iec/libiec_iccp_mod/examples/mms_client_example1/mms_client_example1+0x48e38c)
    #6 0x57b266 in read /usr/include/x86_64-linux-gnu/bits/unistd.h:44
    #7 0x57b266 in Socket_read /root/libiec_iccp_mod/src/hal/socket/linux/socket_linux.c:309
    #8 0x5e98cc in ByteStream_readOctets /root/libiec_iccp_mod/src/common/byte_stream.c:108
    #9 0x5a128d in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:577
    #10 0x5a128d in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #11 0x5a13df in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:590
    #12 0x5a13df in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #13 0x5a13df in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:590
    #14 0x5a13df in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #15 0x5a35df in addPayloadToBuffer /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:590
    #16 0x5a35df in parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:630
    #17 0x5a35df in CotpConnection_parseIncomingMessage /root/libiec_iccp_mod/src/mms/iso_cotp/cotp.c:650
    #18 0x522dac in IsoClientConnection_associate /root/libiec_iccp_mod/src/mms/iso_client/impl/iso_client_connection.c:382
    #19 0x514885 in MmsConnection_connect /root/libiec_iccp_mod/src/mms/iso_mms/client/mms_client_connection.c:887
    #20 0x5113e4 in main /root/temp/iec/libiec_iccp_mod/examples/mms_client_example1/mms_client_example1.c:38:6
    #21 0x7f9d34dc982f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/../csu/libc-start.c:291
    #22 0x41a1c8 in _start (/root/temp/iec/libiec_iccp_mod/examples/mms_client_example1/mms_client_example1+0x41a1c8)
```

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant