New issue

Jump to bottom

Null pointer dereference bug #417

Open **5hadowblad3** opened this issue on Aug 9, 2019 · 0 comments

Assignees

Labels fuzzing

5hadowblad3 commented on Aug 9, 2019

There is a null pointer dereference bug running mp42aac.
It is similar to #413.

Distributor ID: Ubuntu
Description: Ubuntu 16.04.6 LTS
Release: 16.04
Codename: xenial
gcc: 5.4.0

To reproduce the bug,
compile the project with flag
DCMAKE_C_FLAGS=-g -m32 -fsanitize=address,undefined

then run:
./mp42aac input /dev/null

The reason for this problem is due to the mishandled memory allocation:

```
81 AP4_HvccAtom*
82 AP4_HvccAtom::Create(AP4_Size size, AP4_ByteStream& stream)
83 {
84     // read the raw bytes in a buffer
85     unsigned int payload_size = size-AP4_ATOM_HEADER_SIZE;
86     AP4_DataBuffer payload_data(payload_size);
87     AP4_Result result = stream.Read(payload_data.UseData(), payload_size);
88     if (AP4_FAILED(result)) return NULL;
89
90     return new AP4_HvccAtom(size, payload_data.GetData());
91 }
```

payload_data is a null pointer due to allocation failure

directly dereference at the second line

Here is the trace reported by ASAN:
/mnt/data/playground/mp42-a/Source/C++/Core/Ap4DataBuffer.cpp:175:41: runtime error: null pointer passed as argument 1, which is declared to never be null
/usr/include/i386-linux-gnu/bits/string3.h:53:71: runtime error: null pointer passed as argument 1, which is declared to never be null
==147453==WARNING: AddressSanitizer failed to allocate 0xffffffff8 bytes
==147453==AddressSanitizer's allocator is terminating the process instead of returning 0
==147453==If you don't like this behavior set allocator_may_return_null=1
==147453==AddressSanitizer CHECK failed: ../../../../../src/libsanitizer/sanitizer_common/sanitizer_allocator.cc:147 "((0)) != (0)" (0x0, 0x0)
#0 0xf72aa797 (/usr/lib32/libasan.so.2+0x9f797)
#1 0xf72afa69 in __sanitizer::CheckFailed(char const*, int, char const*, unsigned long long, unsigned long long) (/usr/lib32/libasan.so.2+0xa4a69)
#2 0xf722107b (/usr/lib32/libasan.so.2+0x1607b)
#3 0xf72ade80 (/usr/lib32/libasan.so.2+0xa2e80)
#4 0xf7226229 (/usr/lib32/libasan.so.2+0x1b229)
#5 0xf72a2e16 in operator new[](unsigned int) (/usr/lib32/libasan.so.2+0x97e16)
#6 0x877ebaf in AP4_DataBuffer::AP4_DataBuffer(unsigned int) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4DataBuffer.cpp:55
#7 0x889fddb in AP4_HvccAtom::Create(unsigned int, AP4_ByteStream&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4HvccAtom.cpp:86
#8 0x82dc364 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:488
#9 0x82fa1f7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225
#10 0x82fa1f7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:151
#11 0x809a044 in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4File.cpp:104
#12 0x809a044 in AP4_File::AP4_File(AP4_ByteStream&, bool) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4File.cpp:78
#13 0x8082ce7 in main /mnt/data/playground/mp42-a/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:250
#14 0xf6a2b636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)
#15 0x808df1b (/mnt/data/playground/mp42-patch/Build/mp42aac+0x808df1b)

This is the POC input:
poc_input7.zip

barbibulle self-assigned this on Aug 25, 2019

barbibulle added the fuzzing label on Aug 25, 2019

Assignees
barbibulle

Labels
fuzzing

Projects
None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants