New issue

Jump to bottom

Buffer overflow in Ap4ElstAtom.cpp #414

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

Assignees

Labels fuzzing

5hadowblad3 commented on Aug 9, 2019

There is a buffer overflow in Ap4ElstAtom.cpp related to AP4_ElstAtom.

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
```

This is the trace reported by ASAN:
==89902==ERROR: AddressSanitizer: heap-buffer-overflow on address 0xf4b00b64 at pc 0x086bc1e3 bp 0xff8c68b8 sp 0xff8c68a8
WRITE of size 20 at 0xf4b00b64 thread T0
#0 0x86bc1e2 in AP4_Array<AP4_ElstEntry>::Append(AP4_ElstEntry const&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ElstAtom.cpp:88
#1 0x86bc1e2 in AP4_ElstAtom::AP4_ElstAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ElstAtom.cpp:84
#2 0x86bccb5 in AP4_ElstAtom::Create(unsigned int, AP4_ByteStream&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ElstAtom.cpp:51
#3 0x82e1ccc 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:549
#4 0x8301ca3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225
#5 0x82b6bae in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:194
#6 0x82b6bae in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:139
#7 0x82be680 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:88
#8 0x82dc711 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:768
#9 0x8301ca3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225
#10 0x82b6bae in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:194
#11 0x82b6bae in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:139
#12 0x901195b in AP4_TrakAtom::AP4_TrakAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4TrakAtom.cpp:165
#13 0x82da849 in AP4_TrakAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4TrakAtom.h:58
#14 0x82da849 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:383
#15 0x8301ca3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225
#16 0x82b6bae in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:194
#17 0x82b6bae in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:139
#18 0x841a898 in AP4_MoovAtom::AP4_MoovAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4MoovAtom.cpp:80
#19 0x82e2631 in AP4_MoovAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4MoovAtom.h:56
#20 0x82e2631 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:363
#21 0x82fa1f7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225
#22 0x82fa1f7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:151
#23 0x809a044 in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4File.cpp:104
#24 0x809a044 in AP4_File::AP4_File(AP4_ByteStream&, bool) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4File.cpp:78
#25 0x8082ce7 in main /mnt/data/playground/mp42-a/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:250
#26 0xf6a6d636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)
#27 0x808df1b (/mnt/data/playground/mp42-patch/Build/mp42aac+0x808df1b)

```
0xf4b00b64 is located 0 bytes to the right of 20-byte region [0xf4b00b50,0xf4b00b64)
allocated by thread T0 here:
#0 0xf72e4cd6 in operator new(unsigned int) (/usr/lib32/libasan.so.2+0x97cd6)
#1 0x86b7892 in AP4_Array<AP4_ElstEntry>::EnsureCapacity(unsigned int) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4Array.h:172
#2 0x86b7892 in AP4_ElstAtom::AP4_ElstAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ElstAtom.cpp:73
#3 0x86bccb5 in AP4_ElstAtom::Create(unsigned int, AP4_ByteStream&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ElstAtom.cpp:51
#4 0x82e1ccc 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:549
#5 0x8301ca3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225
#6 0x82b6bae in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:194
#7 0x82b6bae in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-
a/Source/C++/Core/Ap4ContainerAtom.cpp:139
#8 0x82be680 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-
a/Source/C++/Core/Ap4ContainerAtom.cpp:88
#9 0x82dc711 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:768
#10 0x8301ca3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225
#11 0x82b6bae in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:194
#12 0x82b6bae in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-
a/Source/C++/Core/Ap4ContainerAtom.cpp:139
#13 0x901195b in AP4_TrakAtom::AP4_TrakAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4TrakAtom.cpp:165
#14 0x82da849 in AP4_TrakAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4TrakAtom.h:58
#15 0x82da849 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:383
#16 0x8301ca3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225
#17 0x82b6bae in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:194
#18 0x82b6bae in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-
a/Source/C++/Core/Ap4ContainerAtom.cpp:139
#19 0x841a898 in AP4_MoovAtom::AP4_MoovAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4MoovAtom.cpp:80
#20 0x82e2631 in AP4_MoovAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4MoovAtom.h:56
#21 0x82e2631 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:363
#22 0x82fa1f7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225
#23 0x82fa1f7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:151
#24 0x809a044 in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4File.cpp:104
#25 0x809a044 in AP4_File::AP4_File(AP4_ByteStream&, bool) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4File.cpp:78
#26 0x8082ce7 in main /mnt/data/playground/mp42-a/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:250
#27 0xf6a6d636 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18636)

SUMMARY: AddressSanitizer: heap-buffer-overflow /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ElstAtom.cpp:88 AP4_Array<AP4_ElstEntry>::Append(AP4_ElstEntry const&)
Shadow bytes around the buggy address:
0x3e960110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3e960120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3e960130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3e960140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3e960150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x3e960160: fa fa fa fa fa fa fa fa fa 00 00[04]fa fa fa
0x3e960170: 00 00 04 fa fa fa 00 00 00 00 fa fa 00 00 00 00
0x3e960180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3e960190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3e9601a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x3e9601b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Heap right redzone: fb
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack partial redzone: f4
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
==89902==ABORTING
```

The reason is that the program does not handle the -m32 complier flag and still let the program read the string in 64bit manner and cause the overwrite.

```
77          if (version == 0) {
78              AP4_UI32 segment_duration;
79              AP4_UI32 media_time;
80              stream.ReadUI32(segment_duration);
81              stream.ReadUI32(media_time);
82              stream.ReadUI16(media_rate);
83              stream.ReadUI16(zero);
84              m_Entries.Append(AP4_ElstEntry(segment_duration, (AP4_SI32)media_time, media_rate));
85          } else {
86              AP4_UI64 segment_duration;
87              AP4_UI64 media_time;
88              stream.ReadUI64(segment_duration);
89              stream.ReadUI64(media_time);
90              stream.ReadUI16(media_rate);
91              stream.ReadUI16(zero);
92              m_Entries.Append(AP4_ElstEntry(segment_duration, (AP4_SI64)media_time, media_rate));
93          }
94      }
95  }
```

Here is the Poc input:
poc_input5.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