

New issue

[Jump to bottom](#)

Heap buffer overflow in AP4_CttsAtom::AP4_CttsAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&) #507

Closed natalie13m opened this issue on May 16, 2020 · 2 comments

Assignees



Labels

fuzzing

natalie13m commented on May 16, 2020 • edited

I use my fuzzing project framework to find some vulnerabilities in mp42aac with command line:
mp42aac @@ /tmp/out.aac
I found a heap buffer overflow in AP4_CttsAtom::AP4_CttsAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&).

Information provided by address sanitizer

[illegible]

[illegible]

#98 0x5d42b2 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:796:20

#99 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:233:14

#100 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4ContainerAtom.cpp:194:12

#101 0x60d6ee in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4ContainerAtom.cpp:139:5

#102 0x60d6ee in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4ContainerAtom.cpp:88

#103 0x5d42b2 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:796:20

#104 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:233:14

#105 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4ContainerAtom.cpp:194:12

#106 0x60e126 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4ContainerAtom.cpp:139:5

#107 0x5a3e4b in AP4_TrakAtom::AP4_TrakAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4TrakAtom.cpp:165:5

#108 0x5d37f8 in AP4_TrakAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4TrakAtom.h:58:20

#109 0x5d37f8 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:399

#110 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:233:14

#111 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4ContainerAtom.cpp:194:12

#112 0x60e126 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4ContainerAtom.cpp:139:5

#113 0x57ccec in AP4_MoovAtom::AP4_MoovAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4MoovAtom.cpp:79:5

#114 0x5d4251 in AP4_MoovAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4MoovAtom.h:56:20

#115 0x5d4251 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:379

#116 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:233:14

#117 0x5d21eb in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:153:12

#118 0x57920e in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4File.cpp:104:12

#119 0x5797bb in AP4_File::AP4_File(AP4_ByteStream&, bool) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4File.cpp:78:5

#120 0x571465 in main /home/natalie/Downloads/Bento4-master/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:250:22

#121 0x7f479e6fc1e2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x271e2)

#122 0x45c96d in _start (/home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac-asan+0x45c96d)

0x607000001180 is located 0 bytes to the right of 80-byte region [0x607000001130,0x607000001180)
allocated by thread T0 here:
#0 0x56de20 in operator new[][(unsigned long) /home/natalie/Research/LLVM/src/llvm-8.0.1.src/projects/compiler-rt/lib/asan/asan_new_delete.cc:109:3
#1 0x6110ed in AP4_CttsAtom::AP4_CttsAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4CttsAtom.cpp:80:29
#2 0x60fce2 in AP4_CttsAtom::Create(unsigned int, AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4CttsAtom.cpp:52:16
#3 0x5d310c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:479:20
#4 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#5 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:194:12
#6 0x60d6ee in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:139:5
#7 0x60d6ee in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:88
#8 0x5d42b2 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:796:20
#9 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#10 0x61bf3d in AP4_DrefAtom::AP4_DrefAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4DrefAtom.cpp:84:16
#11 0x61b922 in AP4_DrefAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4DrefAtom.cpp:50:16
#12 0x5d4fd8 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:560:20
#13 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#14 0x60e27d in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:194:12
#15 0x60d6ee in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:139:5
#16 0x60d6ee in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:88
#17 0x5d42b2 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:796:20
#18 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#19 0x61bf3d in AP4_DrefAtom::AP4_DrefAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4DrefAtom.cpp:84:16
#20 0x61b922 in AP4_DrefAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4DrefAtom.cpp:50:16
#21 0x5d4fd8 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:560:20
#22 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#23 0x61bf3d in AP4_DrefAtom::AP4_DrefAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4DrefAtom.cpp:84:16
#24 0x61b922 in AP4_DrefAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4DrefAtom.cpp:50:16
#25 0x5d4fd8 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:560:20
#26 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#27 0x60e27d in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:194:12
#28 0x60d6ee in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:139:5
#29 0x60d6ee in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:88
#30 0x5d42b2 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:796:20
#31 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#32 0x61bf3d in AP4_DrefAtom::AP4_DrefAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4DrefAtom.cpp:84:16

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4Utils.h:78:22 in AP4_BytesToUInt32BE(unsigned char const*)

Shadow bytes around the buggy address:

0x0c0e7fff81e0: 00 00 00 00 00 00 00 00 00 00 fa fa fa 00 00
0x0c0e7fff81f0: 00 00 00 00 00 00 00 00 00 fa fa fa 00 00 00 00
0x0c0e7fff8200: 00 00 00 00 00 00 00 fa fa fa 00 00 00 00 00 00
0x0c0e7fff8210: 00 00 00 00 fa fa fa 00 00 00 00 00 00 00
0x0c0e7fff8220: 00 fa fa fa fa 00 00 00 00 00 00 00 00 00 00
=>0x0c0e7fff8230:[fa]fa fa fa fa fa fa fa fa fa fa fa
0x0c0e7fff8240: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0e7fff8250: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0e7fff8260: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0e7fff8270: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c0e7fff8280: 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

Freed heap region: fd

Stack left redzone: f1

Stack mid redzone: f2

Stack right redzone: f3

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

Left alloca redzone: ca

Right alloca redzone: cb

Shadow gap: cc

==21708==ABORTING

Information provided by crashwalk

---CRASH SUMMARY---

Filename: psym-crashes/id:000382,sig:06,src:005991,op:flip1,pos:3837

SHA1: 5c2e8caa3c148bb05c322da182cadbc2072fb82e

Classification: UNKNOWN

Hash: f937118ff00ccff334602ba62160ed8c.1396527138624a36d1c970a348bf5074

Command: ./mp42aac psym-crashes/id:000382,sig:06,src:005991,op:flip1,pos:3837 /tmp/out.aac

Faulting Frame:

AP4_CttsAtom::AP4_CttsAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&) @ 0x00055555555dc14a: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

Disassembly:

0x00005555555dc134: mov rcx,QWORD PTR [rbx+0x38]

0x00005555555dc138: lea rsi,[rax+0x8]

0x00005555555dc140: xor eax,eax

0x00005555555dc142: nop WORD PTR [rax+rax1+0x0]

0x00005555555dc148: mov edx,eax

=> 0x00005555555dc14a: mov edx,DWORD PTR [rbp+rdx1+0x0]

0x00005555555dc14e: bswap edx

0x00005555555dc150: mov DWORD PTR [rcx+rax1],edx

0x00005555555dc153: lea edx,[rax+0x4]

0x00005555555dc156: mov edx,DWORD PTR [rbp+rdx*1+0x0]

Stack Head (105 entries):

AP4_CttsAtom::AP4_CttsAto @ 0x00005555555dc14a: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_CttsAtom::Create(unsig @ 0x00005555555dc286: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_AtomFactory::CreateAt @ 0x00005555555cb9c8: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_AtomFactory::CreateAt @ 0x00005555555cddb9c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_ContainerAtom::ReadCh @ 0x00005555555db882: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_ContainerAtom::Create @ 0x00005555555dbbfd: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_AtomFactory::CreateAt @ 0x00005555555cb892: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_AtomFactory::CreateAt @ 0x00005555555cddb9c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_DrefAtom::AP4_DrefAto @ 0x00005555555df391: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_DrefAtom::Create(unsig @ 0x00005555555df47e: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_AtomFactory::CreateAt @ 0x00005555555cb8c7: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_AtomFactory::CreateAt @ 0x00005555555cddb9c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_ContainerAtom::ReadCh @ 0x00005555555db882: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_ContainerAtom::Create @ 0x00005555555dbbfd: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_AtomFactory::CreateAt @ 0x00005555555cb892: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4_AtomFactory::CreateAt @ 0x00005555555cddb9c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

Registers:

rax=0x000000000000091e0 rbx=0x00005555555657dd0 rcx=0x00007ffb7a55010 rdx=0x000000000000091e0

rsi=0x0000000400000050 rdi=0x00005555555652480 rbp=0x00005555555657e20 rsp=0x00007fffffb220

r8=0x0000000000000050 r9=0x0000000000000000 r10=0x0000000000000022 r11=0x00007ffffd93be0

r12=0x000055555556535a0 r13=0x00005555555638208 r14=0x00007ffb7a55010 r15=0x000055555556535a0

rip=0x00005555555dc14a efl=0x00000000000010202 cs=0x0000000000000033 ss=0x000000000000002b

ds=0x0000000000000000 es=0x0000000000000000 fs=0x0000000000000000 gs=0x0000000000000000

Extra Data:

Description: Access violation on source operand

Short description: SourceAv (19/22)

Explanation: The target crashed on an access violation at an address matching the source operand of the current instruction. This likely indicates a read access violation.


---END SUMMARY---

barbille commented on May 17, 2020

Contributor


@natalie13m Thanks for the report. Would it be possible to attach to your fuzz reports the input file that can be used to replicate the problem and fix it?

  **barbibulle** self-assigned this on May 17, 2020

  **barbibulle** added the **fuzzing** label on May 17, 2020

natalie13m commented on May 18, 2020 • edited

Author

 **@natalie13m** Thanks for the report. Would it be possible to attach to your fuzz reports the input file that can be used to replicate the problem and fix it?

Sure. Here is the link of the crash file. I put it in my repository.

<https://github.com/natalie13m/crashes/blob/master/bento4-06c39d9/id:000382%2Csig:06%2Csrc:005991%2Cop:flip1%2Cpos:3837>

 **barbibulle** closed this as completed in **b4a6fd5** on May 21, 2020

Assignees

 **barbibulle**

Labels

fuzzing

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

