New issue

Jump to bottom

Heap-buffer-overflow with ASAN in mp42aac #762

Open 17ssDP opened this issue on Sep 19 · 0 comments

17ssDP commented on Sep 19 • edited

Hi, developers of Bento4:
Thanks for your fix of issue #751
In the test of the binary mp42aac instrumented with ASAN. There are some inputs causing heap-buffer-overflow. Here is the ASAN mode output:

```
==27304==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60300000ed28 at pc
0x0000005a64d9 bp 0x7fffffffb290 sp 0x7fffffffb280
READ of size 1 at 0x60300000ed28 thread T0
#0 0x5a64d8 in AP4_Dec3Atom::AP4_Dec3Atom(unsigned int, unsigned char const*)
/root/Bento4/Source/C++/Core/Ap4Dec3Atom.cpp:161
#1 0x5a6a62 in AP4_Dec3Atom::Create(unsigned int, AP4_ByteStream&)
/root/Bento4/Source/C++/Core/Ap4Dec3Atom.cpp:56
#2 0x508887 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int,
unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:769
#3 0x50ecb6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#4 0x579928 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long
long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#5 0x480e69 in AP4_SampleEntry::Read(AP4_ByteStream&, AP4_AtomFactory&)
/root/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:115
#6 0x480e69 in AP4_AudioSampleEntry::AP4_AudioSampleEntry(unsigned int, unsigned int,
AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:420
#7 0x480e69 in AP4_Eac3SampleEntry::AP4_Eac3SampleEntry(unsigned int, unsigned int, AP4_ByteStream&,
AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:752
#8 0x508d6b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int,
unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:338
#9 0x50ecb6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#10 0x490228 in AP4_StsdAtom::AP4_StsdAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&,
AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:101
#11 0x491bd0 in AP4_StsdAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
/root/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:57
#12 0x50aaae in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int,
unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:458
#13 0x50ecb6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#14 0x577862 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long
long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#15 0x577862 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
#16 0x5785a6 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&,
AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
#17 0x507f53 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int,
unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
#18 0x50ecb6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#19 0x5aea82 in AP4_DrefAtom::AP4_DrefAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&,
AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4DrefAtom.cpp:84
#20 0x5aeff7 in AP4_DrefAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
/root/Bento4/Source/C++/Core/Ap4DrefAtom.cpp:50
#21 0x509882 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int,
```

unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:580
#22 0x50ecb6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#23 0x577862 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#24 0x577862 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
#25 0x5785a6 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
#26 0x507f53 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
#27 0x50ecb6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#28 0x577862 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#29 0x577862 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
#30 0x5785a6 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
#31 0x507f53 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
#32 0x50ecb6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#33 0x577862 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#34 0x577862 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
#35 0x5785a6 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
#36 0x507f53 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
#37 0x50dd7a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#38 0x50dd7a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:154
#39 0x418daf in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) /root/Bento4/Source/C++/Core/Ap4File.cpp:104
#40 0x418daf in AP4_File::AP4_File(AP4_ByteStream&, bool) /root/Bento4/Source/C++/Core/Ap4File.cpp:78
#41 0x4040d7 in main /root/Bento4/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:250
#42 0x7ffff61bb83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
#43 0x408508 in _start (/root/Bento4/mp42aac+0x408508)

```
0x60300000ed28 is located 0 bytes to the right of 24-byte region [0x60300000ed10,0x60300000ed28)
allocated by thread T0 here:
#0 0x7ffff6f03712 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99712)
#1 0x4147b5 in AP4_DataBuffer::AP4_DataBuffer(unsigned int)
/root/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:55
#2 0x17 ()

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/Bento4/Source/C++/Core/Ap4Dec3Atom.cpp:161
AP4_Dec3Atom::AP4_Dec3Atom(unsigned int, unsigned char const*)
Shadow bytes around the buggy address:
0x0c067fff9d50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff9d60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff9d70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff9d80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff9d90: fa fa fa fa fa fa fa fa fa fa fa fa 00 00 00 fa
=>0x0c067fff9da0: fa fa 00 00 00[fa]fa fa 00 00 00 fa fa fa 00 00
0x0c067fff9db0: 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
0x0c067fff9dc0: 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa
0x0c067fff9dd0: fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00
0x0c067fff9de0: 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
0x0c067fff9df0: 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00 00 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
==27304==ABORTING
```

Crash input

https://github.com/17ssDP/fuzzer_crashes/blob/main/Bento4/mp42aac-hbo-00

Validation steps

git clone https://github.com/axiomatic-systems/Bento4
cd Bento4/
mkdir check_build && cd check_build
cmake ../ -DCMAKE_C_COMPILER=clang -DCMAKE_CXX_COMPILER=clang++ -DCMAKE_C_FLAGS="-fsanitize=address" -DCMAKE_CXX_FLAGS="-fsanitize=address" -DCMAKE_BUILD_TYPE=Release
make -j
./mp42aac mp42aac-hbo-00 /dev/null

Environment

Ubuntu 16.04
Clang 10.0.1
gcc 5.5

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant