

[New issue](#)

[Jump to bottom](#)

Heap-buffer-overflow with ASAN in mp42aac #751

✓ Closed

17ssDP opened this issue on Sep 6 · 0 comments

Assignees



Labels

fuzzing

17ssDP commented on Sep 6

Hi, developers of Bento4:

In the test of the binary mp42aac instrumented with ASAN. There are some inputs causing heap-buffer-overflow. Here is the ASAN mode output:

```
=====
==4695==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6190000027a0 at pc 0x7ffff6ef6964
bp 0x7fffffdea0 sp 0x7fffffd648
WRITE of size 4294967288 at 0x6190000027a0 thread T0
#0 0x7ffff6ef6963 in __asan_memcpy (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x8c963)
#1 0x409ed4 in AP4_MemoryByteStream::WritePartial(void const*, unsigned int, unsigned int&)
/home/ferry/dp/Bento4/Source/C++/Core/Ap4ByteStream.cpp:785
#2 0x40d9e3 in AP4_ByteStream::Write(void const*, unsigned int)
/home/ferry/dp/Bento4/Source/C++/Core/Ap4ByteStream.cpp:77
#3 0x4eb601 in AP4_Atom::Write(AP4_ByteStream&)
/home/ferry/dp/Bento4/Source/C++/Core/Ap4Atom.cpp:229
#4 0x4eb601 in AP4_Atom::Clone() /home/ferry/dp/Bento4/Source/C++/Core/Ap4Atom.cpp:316
#5 0x446d7a in AP4_SampleDescription::AP4_SampleDescription(AP4_SampleDescription::Type, unsigned int,
AP4_AtomParent*) /home/ferry/dp/Bento4/Source/C++/Core/Ap4SampleDescription.cpp:138
#6 0x461a8f in AP4_GenericAudioSampleDescription::AP4_GenericAudioSampleDescription(unsigned int,
unsigned int, unsigned short, unsigned short, AP4_AtomParent*)
/home/ferry/dp/Bento4/Source/C++/Core/Ap4SampleDescription.h:259
#7 0x461a8f in AP4_AudioSampleEntry::ToSampleDescription()
/home/ferry/dp/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:630
#8 0x48ca03 in AP4_StsdAtom::GetSampleDescription(unsigned int)
/home/ferry/dp/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:181
#9 0x4040b6 in main /home/ferry/dp/Bento4/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:268
#10 0x7ffff61bb83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
#11 0x408338 in _start (/home/ferry/dp/Bento4/mp42aac+0x408338)

0x6190000027a0 is located 0 bytes to the right of 1056-byte region [0x619000002380,0x6190000027a0)
allocated by thread T0 here:
#0 0x7ffff6f03712 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99712)
#1 0x414c8e in AP4_DataBuffer::ReallocateBuffer(unsigned int)
/home/ferry/dp/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:210
#2 0x414c8e in AP4_DataBuffer::SetBufferSize(unsigned int)
/home/ferry/dp/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:136
#3 0x414c8e in AP4_DataBuffer::Reserve(unsigned int)
/home/ferry/dp/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:107
```

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 __asan_memcpy

Shadow bytes around the buggy address:

0x0c327fff84a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x0c327fff84b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x0c327fff84c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x0c327fff84d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0x0c327fff84e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

=>0x0c327fff84f0: 00 00 00 00[fa]fa fa fa fa fa fa fa fa fa fa

0x0c327fff8500: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

0x0c327fff8510: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

0x0c327fff8520: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

0x0c327fff8530: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

0x0c327fff8540: 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

==4695==ABORTING

Crash input

https://github.com/17ssDP/fuzzer_crashes/blob/main/Bento4/input2

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 input2 /dev/null
```



Environment

Ubuntu 16.04

Clang 10.0.1

gcc 5.5

  **barbibulle** self-assigned this on Sep 18

  **barbibulle** added the **fuzzing** label on Sep 18

 **barbibulle** closed this as completed in [5b7cc25](#) on Sep 18

  **17ssDP** mentioned this issue on Sep 19

Heap-buffer-overflow with ASAN in mp42aac #762

 **Open**

 **glenn guy** pushed a commit to glenn guy/Bento4 that referenced this issue on Oct 2



fix [axiomatic-systems#751](#)

4b8c20c

 **glenn guy** pushed a commit to glenn guy/Bento4 that referenced this issue on Oct 2



fix [axiomatic-systems#751](#)

976a2c3

 **glenn guy** pushed a commit to glenn guy/Bento4 that referenced this issue on Oct 2



fix [axiomatic-systems#751](#)

7a85d7a

 **glenn guy** pushed a commit to xbmc/Bento4 that referenced this issue on Oct 2



fix [axiomatic-systems#751](#)


1565b65

  **17ssDP** mentioned this issue on Oct 4

Heap-buffer-overflow with ASAN in mp42aac #789

 Open

Assignees

 barbibulle

Labels

fuzzing

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants