New issue

Jump to bottom

Heap-buffer-overflow with ASAN in mp42aac #789

Open **17ssDP** opened this issue on Oct 4 · 0 comments

17ssDP commented on Oct 4

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. This issue may be because of an incomplete fix of #751.

```
=================================================================
==8242==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000002798 at pc
0x7f30ba3a2964 bp 0x7fff5a52d110 sp 0x7fff5a52c8b8
WRITE of size 4294967288 at 0x619000002798 thread T0
#0 0x7f30ba3a2963 in __asan_memcpy (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x8c963)
#1 0x409c09 in AP4_MemoryByteStream::WritePartial(void const*, unsigned int, unsigned int&)
/root/Bento4/Source/C++/Core/Ap4ByteStream.cpp:785
#2 0x40da09 in AP4_ByteStream::Write(void const*, unsigned int)
/root/Bento4/Source/C++/Core/Ap4ByteStream.cpp:77
#3 0x65a86f in AP4_SgpdAtom::WriteFields(AP4_ByteStream&)
/root/Bento4/Source/C++/Core/Ap4SgpdAtom.cpp:144
#4 0x4e99bc in AP4_Atom::Write(AP4_ByteStream&) /root/Bento4/Source/C++/Core/Ap4Atom.cpp:229
#5 0x4e99bc in AP4_Atom::Clone() /root/Bento4/Source/C++/Core/Ap4Atom.cpp:316
#6 0x574024 in AP4_ContainerAtom::Clone() /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:172
#7 0x574024 in AP4_ContainerAtom::Clone() /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:172
#8 0x446e72 in AP4_SampleDescription::AP4_SampleDescription(AP4_SampleDescription::Type, unsigned int,
AP4_AtomParent*) /root/Bento4/Source/C++/Core/Ap4SampleDescription.cpp:138
#9 0x460bf8 in AP4_GenericAudioSampleDescription::AP4_GenericAudioSampleDescription(unsigned int,
unsigned int, unsigned short, unsigned short, AP4_AtomParent*)
/root/Bento4/Source/C++/Core/Ap4SampleDescription.h:259
#10 0x460bf8 in AP4_AudioSampleEntry::ToSampleDescription()
/root/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:630
#11 0x4899a4 in AP4_StsdAtom::GetSampleDescription(unsigned int)
/root/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:181
#12 0x404135 in main /root/Bento4/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:268
#13 0x7f30b966783f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
#14 0x408128 in _start (/root/Bento4/mp42aac+0x408128)

0x619000002798 is located 0 bytes to the right of 1048-byte region [0x619000002380,0x619000002798)
allocated by thread T0 here:
#0 0x7f30ba3af712 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99712)
#1 0x4151ce in AP4_DataBuffer::ReallocateBuffer(unsigned int)
/root/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:210
#2 0x4151ce in AP4_DataBuffer::SetBufferSize(unsigned int)
/root/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:136
#3 0x4151ce in AP4_DataBuffer::Reserve(unsigned int)
/root/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[fa]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
==8242==ABORTING

Crash input

https://github.com/17ssDP/fuzzer_crashes/blob/main/Bento4/mp42aac-hbo-01

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-01 /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