axiomatic-systems / **Bento4** Public

Code Issues 421 Pull requests 27 Actions Projects Wiki ...

New issue Jump to bottom

Heap-buffer-overflow with ASAN in mp42ts #764

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

17ssDP commented on Sep 19

Hi, developers of Bento4:
In the test of the binary mp42ts instrumented with ASAN. There are some inputs causing heap-buffer-overflow. Here is the ASAN mode output:

```
==10897==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60300000ec3c at pc 0x0000004a9771 bp 0x7fffffffb150 sp 0x7fffffffb140
READ of size 4 at 0x60300000ec3c thread T0
#0 0x4a9770 in AP4_BitReader::SkipBits(unsigned int) /root/Bento4/Source/C++/Core/Ap4Utils.cpp:564
#1 0x53f5c5 in AP4_Dac4Atom::AP4_Dac4Atom(unsigned int, unsigned char const*) /root/Bento4/Source/C++/Core/Ap4Dac4Atom.cpp:396
#2 0x543230 in AP4_Dac4Atom::Create(unsigned int, AP4_ByteStream&) /root/Bento4/Source/C++/Core/Ap4Dac4Atom.cpp:58
#3 0x4f7503 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:776
#4 0x4fc596 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#5 0x51cd08 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#6 0x4826d1 in AP4_SampleEntry::Read(AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:115
#7 0x4826d1 in AP4_AudioSampleEntry::AP4_AudioSampleEntry(unsigned int, unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:420
#8 0x5d736d in AP4_EncaSampleEntry::AP4_EncaSampleEntry(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4Protection.cpp:74
#9 0x4f4a3c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:298
#10 0x4fc596 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#11 0x614618 in AP4_StsdAtom::AP4_StsdAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:101
#12 0x615fc0 in AP4_StsdAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:57
#13 0x4f838e in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:458
#14 0x4fc596 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#15 0x51ac42 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#16 0x51ac42 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
#17 0x51b986 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
#18 0x4f5833 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
#19 0x4fc596 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#20 0x51ac42 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#21 0x51ac42 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
```

```
#22 0x51b986 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
#23 0x4f5833 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
#24 0x4fc596 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#25 0x51ac42 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#26 0x51ac42 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
#27 0x51b986 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
#28 0x4f5833 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
#29 0x4fc596 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#30 0x51ac42 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#31 0x51ac42 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
#32 0x49cfb2 in AP4_TrakAtom::AP4_TrakAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4TrakAtom.cpp:165
#33 0x4f7709 in AP4_TrakAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4TrakAtom.h:58
#34 0x4f7709 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:413
#35 0x4fc596 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#36 0x51ac42 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#37 0x51ac42 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
#38 0x430fac in AP4_MoovAtom::AP4_MoovAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4MoovAtom.cpp:80
#39 0x4f5430 in AP4_MoovAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4MoovAtom.h:56
#40 0x4f5430 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:393
#41 0x4fb65a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#42 0x4fb65a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:154
#43 0x41c6af in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) /root/Bento4/Source/C++/Core/Ap4File.cpp:104
#44 0x41c6af in AP4_File::AP4_File(AP4_ByteStream&, bool) /root/Bento4/Source/C++/Core/Ap4File.cpp:78
#45 0x404446 in main /root/Bento4/Source/C++/Apps/Mp42Ts/Mp42Ts.cpp:511
```

```
#46 0x7ffff61bb83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
#47 0x40ae38 in _start (/root/Bento4/mp42ts+0x40ae38)

0x60300000ec3c is located 0 bytes to the right of 28-byte region [0x60300000ec20,0x60300000ec3c)
allocated by thread T0 here:
#0 0x7ffff6f03712 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99712)
#1 0x419645 in AP4_DataBuffer::ReallocateBuffer(unsigned int)
/root/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:210
#2 0x419645 in AP4_DataBuffer::SetBufferSize(unsigned int)
/root/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:136

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/Bento4/Source/C++/Core/Ap4Utils.cpp:564
AP4_BitReader::SkipBits(unsigned int)
Shadow bytes around the buggy address:
0x0c067fff9d30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff9d40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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 00 00 00[04]fa fa 00 00 00 02 fa fa
0x0c067fff9d90: 00 00 00 02 fa fa 00 00 00 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
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
==10897==ABORTING
```

Crash input

https://github.com/17ssDP/fuzzer_crashes/blob/main/Bento4/mp42ts-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
./mp42ts mp42ts-hbo-00 /dev/null
```

Environment

Ubuntu 16.04
Clang 10.0.1
gcc 5.5

17ssDP mentioned this issue on Oct 4

Heap-buffer-overflow with ASAN in mp42ts #787

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant