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 #787

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

17ssDP commented on Oct 4

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. The output is different from #764

```
=================================================================
==3902==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60400000df38 at pc
0x0000004a51a6 bp 0x7ffc109910f0 sp 0x7ffc109910e0
READ of size 1 at 0x60400000df38 thread T0
#0 0x4a51a5 in AP4_BitReader::ReadCache() const /root/Bento4/Source/C++/Core/Ap4Utils.cpp:447
#1 0x4a51a5 in AP4_BitReader::ReadBits(unsigned int) /root/Bento4/Source/C++/Core/Ap4Utils.cpp:467
#2 0x5405fc in AP4_Dac4Atom::AP4_Dac4Atom(unsigned int, unsigned char const*)
/root/Bento4/Source/C++/Core/Ap4Dac4Atom.cpp:313
#3 0x5423a2 in AP4_Dac4Atom::Create(unsigned int, AP4_ByteStream&)
/root/Bento4/Source/C++/Core/Ap4Dac4Atom.cpp:58
#4 0x4f47c5 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int,
unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:776
#5 0x4f955a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#6 0x51a25e in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long
long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#7 0x487d31 in AP4_SampleEntry::Read(AP4_ByteStream&, AP4_AtomFactory&)
/root/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:115
#8 0x487d31 in AP4_AudioSampleEntry::AP4_AudioSampleEntry(unsigned int, unsigned int,
AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:420
#9 0x487d31 in AP4_Ac4SampleEntry::AP4_Ac4SampleEntry(unsigned int, unsigned int, AP4_ByteStream&,
AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:801
#10 0x4f1aad in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int,
unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:342
#11 0x4f955a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#12 0x6134a9 in AP4_StsdAtom::AP4_StsdAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&,
AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:101
#13 0x61534b in AP4_StsdAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
/root/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:57
#14 0x4f55a6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int,
unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:458
#15 0x4f955a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#16 0x5181d5 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long
long) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
#17 0x5181d5 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
#18 0x518fce in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&,
AP4_AtomFactory&) /root/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
#19 0x4f2b69 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int,
unsigned long long, AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
#20 0x4f865c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
#21 0x4f865c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&)
/root/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:154
```

```
#22 0x41c87f in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) /root/Bento4/Source/C++/Core/Ap4File.cpp:104
#23 0x41c87f in AP4_File::AP4_File(AP4_ByteStream&, bool) /root/Bento4/Source/C++/Core/Ap4File.cpp:78
#24 0x40441f in main /root/Bento4/Source/C++/Apps/Mp42Ts/Mp42Ts.cpp:511
#25 0x7fb1c343783f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
#26 0x40ad98 in _start (/root/Bento4/mp42ts+0x40ad98)

0x60400000df38 is located 0 bytes to the right of 40-byte region [0x60400000df10,0x60400000df38)
allocated by thread T0 here:
#0 0x7fb1c417f712 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99712)
#1 0x4199e5 in AP4_DataBuffer::ReallocateBuffer(unsigned int) /root/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:210
#2 0x4199e5 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:447
AP4_BitReader::ReadCache() const
Shadow bytes around the buggy address:
0x0c087fff9b90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff9ba0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff9bb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff9bc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff9bd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c087fff9be0: fa fa 00 00 00 00 00[fa]fa fa 00 00 00 00 06 fa
0x0c087fff9bf0: fa fa 00 00 00 00 06 fa fa fa 00 00 00 00 00 00
0x0c087fff9c00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff9c10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff9c20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff9c30: 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
==3902==ABORTING
```

Crash input

https://github.com/17ssDP/fuzzer_crashes/blob/main/Bento4/mp42ts-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
./mp42ts mp42ts-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