axiomatic-systems / **Bento4** Public

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

New issue Jump to bottom

Memory leaks with ASAN in mp42aac #763

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 mp42aac instrumented with ASAN. There are some inputs causing memory leaks.
Here is the ASAN mode output:

```
=================================================================
==19530==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 80 byte(s) in 1 object(s) allocated from:
#0 0x7ffff6f03592 in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99592)
#1 0x5ad493 in AP4_DescriptorFactory::CreateDescriptorFromStream(AP4_ByteStream&, AP4_Descriptor*&)
/root/Bento4/Source/C++/Core/Ap4DescriptorFactory.cpp:85

Indirect leak of 112 byte(s) in 2 object(s) allocated from:
#0 0x7ffff6f03592 in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99592)
#1 0x5ad7a9 in AP4_DescriptorFactory::CreateDescriptorFromStream(AP4_ByteStream&, AP4_Descriptor*&)
/root/Bento4/Source/C++/Core/Ap4DescriptorFactory.cpp:127

Indirect leak of 72 byte(s) in 3 object(s) allocated from:
#0 0x7ffff6f03592 in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99592)
#1 0x604f8b in AP4_List<AP4_Descriptor>::Add(AP4_Descriptor*)
/root/Bento4/Source/C++/Core/Ap4List.h:160
#2 0x604f8b in AP4_ObjectDescriptor::AP4_ObjectDescriptor(AP4_ByteStream&, unsigned char, unsigned int,
unsigned int) /root/Bento4/Source/C++/Core/Ap4ObjectDescriptor.cpp:103

Indirect leak of 32 byte(s) in 1 object(s) allocated from:
#0 0x7ffff6f03592 in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99592)
#1 0x5ad532 in AP4_DescriptorFactory::CreateDescriptorFromStream(AP4_ByteStream&, AP4_Descriptor*&)
/root/Bento4/Source/C++/Core/Ap4DescriptorFactory.cpp:115
```

```
Indirect leak of 25 byte(s) in 2 object(s) allocated from:
#0 0x7ffff6f03712 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99712)
#1 0x415b81 in AP4_DataBuffer::ReallocateBuffer(unsigned int)
/root/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:210
#2 0x415b81 in AP4_DataBuffer::SetDataSize(unsigned int)
/root/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:151

SUMMARY: AddressSanitizer: 321 byte(s) leaked in 9 allocation(s).
```

Crash Input

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

Verification 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-ml-00 /dev/null
```

Environment

Ubuntu 16.04
Clang 10.0.1
gcc 5.5

17ssDP mentioned this issue on Oct 4

Memory leaks with ASAN in mp42aac #788

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant