New issue

Jump to bottom

Memory leaks with ASAN in mp42ts #750

Open **17ssDP** opened this issue on Sep 6 · 0 comments

17ssDP commented on Sep 6

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

```
=================================================================
==18321==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 48 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 0x4c871d in AP4_StdcFileByteStream::Create(AP4_FileByteStream*, char const*, AP4_FileByteStream::Mode, AP4_ByteStream*&) /home/ferry/dp/chunkfuzzer-evaluation/unibench-latest/Bento4/Source/C++/System/StdC/Ap4StdCFileByteStream.cpp:279
#2 0x4c871d in AP4_FileByteStream::Create(char const*, AP4_FileByteStream::Mode, AP4_ByteStream*&) /home/ferry/dp/chunkfuzzer-evaluation/unibench-latest/Bento4/Source/C++/System/StdC/Ap4StdCFileByteStream.cpp:439

Indirect leak of 72 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 0x404286 in main /home/ferry/dp/chunkfuzzer-evaluation/unibench-latest/Bento4/Source/C++/Apps/Mp42Ts/Mp42Ts.cpp:511
#2 0x7ffff61bb83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)

Indirect leak of 64 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 0x4f57d1 in AP4_RtpAtom::Create(unsigned int, AP4_ByteStream&) /home/ferry/dp/chunkfuzzer-evaluation/unibench-latest/Bento4/Source/C++/Core/Ap4RtpAtom.h:53
#2 0x4f57d1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/ferry/dp/chunkfuzzer-evaluation/unibench-latest/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:689
```

Indirect leak of 24 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 0x4d2591 in AP4_List<AP4_Atom>::Add(AP4_Atom*) /home/ferry/dp/chunkfuzzer-evaluation/unibench-latest/Bento4/Source/C++/Core/Ap4List.h:160
#2 0x4d2591 in AP4_AtomParent::AddChild(AP4_Atom*, int) /home/ferry/dp/chunkfuzzer-evaluation/unibench-latest/Bento4/Source/C++/Core/Ap4Atom.cpp:532

SUMMARY: AddressSanitizer: 208 byte(s) leaked in 4 allocation(s).

Crash Input

https://github.com/17ssDP/fuzzer_crashes/blob/main/Bento4/input1

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
./mp42ts input1 /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