New issue

Jump to bottom

requested allocation size 0xfffffffffffffffd in /Source/C++/Core/Ap4RtpAtom.cpp:49 #703

Open **a4865g** opened this issue on May 8 · 0 comments

a4865g commented on May 8

SUMMARY: AddressSanitizer: requested allocation size 0xfffffffffffffffd in /Source/C++/Core/Ap4RtpAtom.cpp:49

- Version

```
$ ./mp42hls
MP4 To HLS File Converter - Version 1.2
(Bento4 Version 1.6.0.0)
(c) 2002-2018 Axiomatic Systems, LLC
```

branch d02ef82

- Platform

```
$ gcc --version
gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0
Copyright (C) 2019 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

$ uname -r
5.13.0-40-generic

$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.4 LTS
Release:        20.04
Codename:       focal
```

- Steps to reproduce

```
$ mkdir build
$ cd build
$ cmake .. -DCMAKE_CXX_FLAGS="-fsanitize=address -g" -DCMAKE_C_FLAGS="-fsanitize=address -g" -
DCMAKE_EXE_LINKER_FLAGS="-fsanitize=address" -DCMAKE_MODULE_LINKER_FLAGS="-fsanitize=address"
$ make

$ ./mp42hls poc
```

- Asan

```
$ ./mp42hls poc
=================================================================
==2656357==ERROR: AddressSanitizer: requested allocation size 0xfffffffffffffffd (0x800 after
adjustments for alignment, red zones etc.) exceeds maximum supported size of 0x10000000000 (thread
T0)
    #0 0x7f94774c8787 in operator new[](unsigned long)
../../../../src/libsanitizer/asan/asan_new_delete.cc:107
    #1 0x55c100eee930 in AP4_RtpAtom::AP4_RtpAtom(unsigned int, AP4_ByteStream&)
/home/wulearn/Bento4/Source/C++/Core/Ap4RtpAtom.cpp:49
    #2 0x55c100e75f4d in AP4_RtpAtom::Create(unsigned int, AP4_ByteStream&)
(/home/wulearn/Bento4/build/mp42hls+0x352f4d)
    #3 0x55c100e744da in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int,
unsigned int, unsigned long long, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:689
    #4 0x55c100e70f7a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long
long&, AP4_Atom*&) /home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #5 0x55c100e70549 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:154
    #6 0x55c100ea1392 in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool)
/home/wulearn/Bento4/Source/C++/Core/Ap4File.cpp:104
    #7 0x55c100ea0fe0 in AP4_File::AP4_File(AP4_ByteStream&, bool)
/home/wulearn/Bento4/Source/C++/Core/Ap4File.cpp:78
    #8 0x55c100e5bb38 in main /home/wulearn/Bento4/Source/C++/Apps/Mp42Hls/Mp42Hls.cpp:1894
    #9 0x7f9476e9f0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)

==2656357==HINT: if you don't care about these errors you may set allocator_may_return_null=1
SUMMARY: AddressSanitizer: allocation-size-too-big
../../../../src/libsanitizer/asan/asan_new_delete.cc:107 in operator new[](unsigned long)
==2656357==ABORTING
```

poc: poc.zip

Thanks!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant