New issue

Jump to bottom

SEGV on unknown address 0x000000000000 in /Source/C++/Core/Ap4DataBuffer.cpp:175 #708

Open a4865g opened this issue on May 8 · 0 comments

a4865g commented on May 8

SUMMARY: AddressSanitizer: SEGV on unknown address 0x000000000000 in /Source/C++/Core/Ap4DataBuffer.cpp:175

- Version

```
$ ./mp4dump
MP4 File Dumper - Version 1.2
(Bento4 Version 1.6.0.0)
(c) 2002-2011 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

$ ./mp4dump poc
```

- Asan

```
$ ./mp4dump poc
[ftyp] size=8+16
  major_brand = mk24
  minor_version = 24017c
  compatible_brand = yl73
  compatible_brand = oxsh
[free] size=8+0
[mdat] size=8+397
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2476501==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f73f2e09321 bp
0x7fffe8de6b70 sp 0x7fffe8de62e0 T0)
==2476501==The signal is caused by a READ memory access.
==2476501==Hint: address points to the zero page.
    #0 0x7f73f2e09320 in AddressIsPoisoned ../../../../src/libsanitizer/asan/asan_mapping.h:396
    #1 0x7f73f2e09320 in QuickCheckForUnpoisonedRegion
../../../../src/libsanitizer/asan/asan_interceptors_memintrinsics.h:30
    #2 0x7f73f2e09320 in __interceptor_memcpy
../../../../src/libsanitizer/sanitizer_common/sanitizer_common_interceptors.inc:790
    #3 0x55719b16636b in AP4_DataBuffer::SetData(unsigned char const*, unsigned int)
/home/wulearn/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:175
    #4 0x55719b14744a in AP4_AvccAtom::AP4_AvccAtom(unsigned int, unsigned char const*)
/home/wulearn/Bento4/Source/C++/Core/Ap4AvccAtom.cpp:176
    #5 0x55719b1464ab in AP4_AvccAtom::Create(unsigned int, AP4_ByteStream&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AvccAtom.cpp:95
    #6 0x55719b140dc6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int,
unsigned int, unsigned long long, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:513
    #7 0x55719b13e5ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long
long&, AP4_Atom*&) /home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #8 0x55719b15161d in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&,
unsigned long long) /home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
    #9 0x55719b1bfeea in AP4_SampleEntry::Read(AP4_ByteStream&, AP4_AtomFactory&)
/home/wulearn/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:115
    #10 0x55719b1c46f0 in AP4_VisualSampleEntry::AP4_VisualSampleEntry(unsigned int, unsigned int,
AP4_ByteStream&, AP4_AtomFactory&) /home/wulearn/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:884
    #11 0x55719b1c5c2a in AP4_AvcSampleEntry::AP4_AvcSampleEntry(unsigned int, unsigned int,
AP4_ByteStream&, AP4_AtomFactory&) /home/wulearn/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:1136
    #12 0x55719b13f203 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int,
unsigned int, unsigned long long, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:319
    #13 0x55719b13e5ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long
long&, AP4_Atom*&) /home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #14 0x55719b1d5c90 in AP4_StsdAtom::AP4_StsdAtom(unsigned int, unsigned char, unsigned int,
```

```
AP4_ByteStream&, AP4_AtomFactory&) /home/wulearn/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:101
    #15 0x55719b1d550f in AP4_StsdAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
/home/wulearn/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:57
    #16 0x55719b1409a6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int,
unsigned int, unsigned long long, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:458
    #17 0x55719b13e5ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long
long&, AP4_Atom*&) /home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #18 0x55719b15161d in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&,
unsigned long long) /home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
    #19 0x55719b151080 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long,
bool, AP4_ByteStream&, AP4_AtomFactory&)
/home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
    #20 0x55719b150be7 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) /home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
    #21 0x55719b142358 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int,
unsigned int, unsigned long long, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
    #22 0x55719b13e5ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long
long&, AP4_Atom*&) /home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #23 0x55719b15161d in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&,
unsigned long long) /home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
    #24 0x55719b151080 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long,
bool, AP4_ByteStream&, AP4_AtomFactory&)
/home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
    #25 0x55719b150be7 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) /home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
    #26 0x55719b142358 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int,
unsigned int, unsigned long long, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
    #27 0x55719b13e5ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long
long&, AP4_Atom*&) /home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #28 0x55719b15161d in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&,
unsigned long long) /home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
    #29 0x55719b151080 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long,
bool, AP4_ByteStream&, AP4_AtomFactory&)
/home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
    #30 0x55719b150be7 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) /home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88
    #31 0x55719b142358 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int,
unsigned int, unsigned long long, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816
    #32 0x55719b13e5ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long
long&, AP4_Atom*&) /home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #33 0x55719b15161d in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&,
unsigned long long) /home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
    #34 0x55719b151080 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long,
bool, AP4_ByteStream&, AP4_AtomFactory&)
/home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
    #35 0x55719b1eb610 in AP4_TrakAtom::AP4_TrakAtom(unsigned int, AP4_ByteStream&,
AP4_AtomFactory&) /home/wulearn/Bento4/Source/C++/Core/Ap4TrakAtom.cpp:165
    #36 0x55719b143429 in AP4_TrakAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
(/home/wulearn/Bento4/build/mp4dump+0x324429)
    #37 0x55719b14063f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int,
unsigned int, unsigned long long, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:413
```

```
    #38 0x55719b13e5ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long
long&, AP4_Atom*&) /home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #39 0x55719b15161d in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&,
unsigned long long) /home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194
    #40 0x55719b151080 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long,
bool, AP4_ByteStream&, AP4_AtomFactory&)
/home/wulearn/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139
    #41 0x55719b189a6c in AP4_MoovAtom::AP4_MoovAtom(unsigned int, AP4_ByteStream&,
AP4_AtomFactory&) /home/wulearn/Bento4/Source/C++/Core/Ap4MoovAtom.cpp:80
    #42 0x55719b1433bb in AP4_MoovAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
(/home/wulearn/Bento4/build/mp4dump+0x3243bb)
    #43 0x55719b1404b8 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int,
unsigned int, unsigned long long, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:393
    #44 0x55719b13e5ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long
long&, AP4_Atom*&) /home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #45 0x55719b13dbbd in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&)
/home/wulearn/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:154
    #46 0x55719b130115 in main /home/wulearn/Bento4/Source/C++/Apps/Mp4Dump/Mp4Dump.cpp:342
    #47 0x7f73f28540b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
    #48 0x55719b12e8ed in _start (/home/wulearn/Bento4/build/mp4dump+0x30f8ed)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ../../../../src/libsanitizer/asan/asan_mapping.h:396 in
AddressIsPoisoned
==2476501==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