New issue

Jump to bottom

A Segmentation fault in Ap4StszAtom.cpp:154 #540

Open **seviezhou** opened this issue on Jul 31, 2020 · 0 comments

seviezhou commented on Jul 31, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), mp42aac (latest master 174b94)

Configure

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"

Command line

./build/mp42aac ./Bento4/SEGV-GetSampleSize-Ap4StszAtom-154 -o /dev/null

Output

```
Audio Track:
  duration: 3623 ms
  sample count: 2147483726
Segmentation fault (core dumped)
```

AddressSanitizer output

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==64813==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000068ee18 bp 0x7ffd9fff70c0 sp 0x7ffd9fff6ef0 T0)
==64813==The signal is caused by a READ memory access.
==64813==Hint: address points to the zero page.
    #0 0x68ee17 in AP4_StszAtom::GetSampleSize(unsigned int, unsigned int&) /home/seviezhou/Bento4/Source/C++/Core/Ap4StszAtom.cpp:154:27
    #1 0x5b166c in AP4_AtomSampleTable::GetSample(unsigned int, AP4_Sample&) /home/seviezhou/Bento4/Source/C++/Core/Ap4AtomSampleTable.cpp
    #2 0x564f45 in AP4_Track::GetSample(unsigned int, AP4_Sample&) /home/seviezhou/Bento4/Source/C++/Core/Ap4Track.cpp:435:43
    #3 0x564f45 in AP4_Track::ReadSample(unsigned int, AP4_Sample&, AP4_DataBuffer&) /home/seviezhou/Bento4/Source/C++/Core/Ap4Track.cpp:469
    #4 0x51826d in WriteSamples(AP4_Track*, AP4_SampleDescription*, AP4_ByteStream*) /home/seviezhou/Bento4/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:192:12
    #5 0x51826d in main /home/seviezhou/Bento4/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:281
    #6 0x7f7ae36e1b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #7 0x41afc9 in _start (/home/seviezhou/Bento4/build/mp42aac+0x41afc9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/Bento4/Source/C++/Core/Ap4StszAtom.cpp:154:27 in AP4_StszAtom::GetSampleSize(unsigned int, unsigned int&)
==64813==ABORTING
```

POC

SEGV-GetSampleSize-Ap4StszAtom-154.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant