New issue

Jump to bottom

Heap overflow in mp4hls, ReadBits, Ap4Mp4AudioInfo.cpp:66 #806

Open **5hadowblad3** opened this issue on Oct 24 · 0 comments

5hadowblad3 commented on Oct 24

Hi, there.

There is an heap overflow in ReadBits, Ap4Mp4AudioInfo.cpp:66, in the newest master branch `5e7bb34` , which seems to be incomplete fix of issue #194.

Here is the reproducing command:

```
mp42hls poc
```

POC:
mp42hls_ReadBits_Ap4Mp4AudioInfo66.zip
(unzip first)

Here is the reproduce trace reported by ASAN:

```
==64087==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000275 at pc
0x000000511365 bp 0x7fff4cecb370 sp 0x7fff4cecb368
 READ of size 1 at 0x602000000275 thread T0
     #0 0x511364 in AP4_Mp4AudioDsiParser::ReadBits(unsigned int)
/benchmark/Bento4/Source/C++/Codecs/Ap4Mp4AudioInfo.cpp:66:56
     #1 0x511a50 in AP4_Mp4AudioDecoderConfig::ParseExtension(AP4_Mp4AudioDsiParser&)
/benchmark/Bento4/Source/C++/Codecs/Ap4Mp4AudioInfo.cpp:159:20
     #2 0x513cdb in AP4_Mp4AudioDecoderConfig::Parse(unsigned char const*, unsigned int)
/benchmark/Bento4/Source/C++/Codecs/Ap4Mp4AudioInfo.cpp:317:30
     #3 0x5a093c in AP4_Mpeg2TsAudioSampleStream::WriteSample(AP4_Sample&, AP4_DataBuffer&,
AP4_SampleDescription*, bool, AP4_ByteStream&)
/benchmark/Bento4/Source/C++/Core/Ap4Mpeg2Ts.cpp:442:44
     #4 0x50991a in WriteSamples(AP4_Mpeg2TsWriter*, PackedAudioWriter*, AP4_Track*,
SampleReader*, AP4_Mpeg2TsWriter::SampleStream*, AP4_Track*, SampleReader*,
AP4_Mpeg2TsWriter::SampleStream*, unsigned int, unsigned char)
/benchmark/Bento4/Source/C++/Apps/Mp42Hls/Mp42Hls.cpp:1274:40
     #5 0x50991a in main  /benchmark/Bento4/Source/C++/Apps/Mp42Hls/Mp42Hls.cpp:2188:14
```

```
    #6 0x7efd53469082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #7 0x41d8ed in _start ( /benchmark/Bento4/build-a/mp42hls+0x41d8ed)

 0x602000000275 is located 0 bytes to the right of 5-byte region [0x602000000270,0x602000000275)
 allocated by thread T0 here:
    #0 0x4f8017 in operator new[](unsigned long)  /dependence/llvm11/llvm-
11.0.0.src/projects/compiler-rt/lib/asan/asan_new_delete.cpp:102:3
    #1 0x560ebf in AP4_DataBuffer::AP4_DataBuffer(void const*, unsigned int)
/benchmark/Bento4/Source/C++/Core/Ap4DataBuffer.cpp:68:20
    #2 0x5a093c in AP4_Mpeg2TsAudioSampleStream::WriteSample(AP4_Sample&, AP4_DataBuffer&,
AP4_SampleDescription*, bool, AP4_ByteStream&)
/benchmark/Bento4/Source/C++/Core/Ap4Mpeg2Ts.cpp:442:44
    #3 0x50991a in WriteSamples(AP4_Mpeg2TsWriter*, PackedAudioWriter*, AP4_Track*,
SampleReader*, AP4_Mpeg2TsWriter::SampleStream*, AP4_Track*, SampleReader*,
AP4_Mpeg2TsWriter::SampleStream*, unsigned int, unsigned char)
/benchmark/Bento4/Source/C++/Apps/Mp42Hls/Mp42Hls.cpp:1274:40
    #4 0x50991a in main  /benchmark/Bento4/Source/C++/Apps/Mp42Hls/Mp42Hls.cpp:2188:14
    #5 0x7efd53469082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-
start.c:308:16

 SUMMARY: AddressSanitizer: heap-buffer-overflow
/benchmark/Bento4/Source/C++/Codecs/Ap4Mp4AudioInfo.cpp:66:56 in
AP4_Mp4AudioDsiParser::ReadBits(unsigned int)
 Shadow bytes around the buggy address:
   0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   0x0c047fff8000: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa fd fd
   0x0c047fff8010: fa fa 04 fa fa fa fd fd fa fa 00 05 fa fa 05 fa
   0x0c047fff8020: fa fa 06 fa fa fa 00 fa fa fa fd fd fa fa 04 fa
   0x0c047fff8030: fa fa fd fa fa fa fd fa fa fa 01 fa fa fa 00 00
 =>0x0c047fff8040: fa fa 00 00 fa fa 05 fa fa fa 00 04 fa fa[05]fa
   0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c047fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c047fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c047fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c047fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 Shadow byte legend (one shadow byte represents 8 application bytes):
   Addressable:           00
   Partially addressable: 01 02 03 04 05 06 07
   Heap left redzone:       fa
   Freed heap region:       fd
   Stack left redzone:      f1
   Stack mid redzone:       f2
   Stack right redzone:     f3
   Stack after return:      f5
   Stack use after scope:   f8
   Global redzone:          f9
   Global init order:       f6
   Poisoned by user:        f7
   Container overflow:      fc
   Array cookie:            ac
   Intra object redzone:    bb
   ASan internal:           fe
   Left alloca redzone:     ca
   Right alloca redzone:    cb
```

```
  Shadow gap:              cc
==64087==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant