New issue

Jump to bottom

Concurrent heap use after free in mp42hls, GetOffset, Ap4Sample.h:99 #802

Open **5hadowblad3** opened this issue on Oct 19 · 0 comments

5hadowblad3 commented on Oct 19

Hi, there.

There is an heap overflow in mp42hls, GetOffset, Ap4Sample.h:99, in the newest commit `5e7bb34` . This seems to be an incomplete fix of issue #461.

Here is the reproducing command:

```
./mp42hls poc
```

POC:
mp42hls_cuaf_Ap4Sample99.zip
(unzip first)

Here is the reproduce trace reported by ASAN:

```
==2007234==ERROR: AddressSanitizer: heap-use-after-free on address 0x604000005dd8 at pc
0x0000005852ab bp 0x7ffc127b7960 sp 0x7ffc127b7958
 READ of size 8 at 0x604000005dd8 thread T0
     #0 0x5852aa in AP4_Sample::GetOffset() const
/benchmark/Bento4/Source/C++/Core/Ap4Sample.h:99:48
     #1 0x5852aa in AP4_LinearReader::Advance(bool)
/benchmark/Bento4/Source/C++/Core/Ap4LinearReader.cpp:434:54
     #2 0x585ab1 in AP4_LinearReader::ReadNextSample(unsigned int, AP4_Sample&, AP4_DataBuffer&)
/benchmark/Bento4/Source/C++/Core/Ap4LinearReader.cpp:530:29
     #3 0x509a31 in ReadSample(SampleReader&, AP4_Track&, AP4_Sample&, AP4_DataBuffer&, double&,
double&, bool&)  /benchmark/Bento4/Source/C++/Apps/Mp42Hls/Mp42Hls.cpp:1004:32
     #4 0x509a31 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:1289:22
     #5 0x509a31 in main  /benchmark/Bento4/Source/C++/Apps/Mp42Hls/Mp42Hls.cpp:2188:14
     #6 0x7f33bacb6082 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)

 0x604000005dd8 is located 8 bytes inside of 48-byte region [0x604000005dd0,0x604000005e00)
 freed by thread T0 here:
    #0 0x4f88b7 in operator delete(void*)  /dependence/llvm11/llvm-11.0.0.src/projects/compiler-
rt/lib/asan/asan_new_delete.cpp:160:3
    #1 0x584f07 in AP4_LinearReader::SampleBuffer::~SampleBuffer()
/benchmark/Bento4/Source/C++/Core/Ap4LinearReader.h:104:26
    #2 0x584f07 in AP4_LinearReader::Advance(bool)
/benchmark/Bento4/Source/C++/Core/Ap4LinearReader.cpp:462:17

 previously allocated by thread T0 here:
    #0 0x4f7eb7 in operator new(unsigned long)  /dependence/llvm11/llvm-
11.0.0.src/projects/compiler-rt/lib/asan/asan_new_delete.cpp:99:3
    #1 0x584892 in AP4_LinearReader::Advance(bool)
/benchmark/Bento4/Source/C++/Core/Ap4LinearReader.cpp:422:41

 SUMMARY: AddressSanitizer: heap-use-after-free
/benchmark/Bento4/Source/C++/Core/Ap4Sample.h:99:48 in AP4_Sample::GetOffset() const
 Shadow bytes around the buggy address:
   0x0c087fff8b60: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fd
   0x0c087fff8b70: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fd
   0x0c087fff8b80: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fd
   0x0c087fff8b90: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fd
   0x0c087fff8ba0: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fd
 =>0x0c087fff8bb0: fa fa fd fd fd fd fd fa fa fa fd[fd]fd fd fd fd
   0x0c087fff8bc0: fa fa fd fd fd fd fd fa fa fa fa fa fa fa fa fa
   0x0c087fff8bd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c087fff8be0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c087fff8bf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c087fff8c00: 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
 ==2007234==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant