New issue

Jump to bottom

# SEGV by a READ memory access in AP4_DecoderConfigDescriptor::WriteFields #509

Open natalie13m opened this issue on May 16, 2020 · 1 comment

Assignees

Labels fuzzing

**natalie13m** commented on May 16, 2020 • edited

## Command line:

./mp42aac @@ /tmp/out.aac

## Information provided by crashwalk:

```
---CRASH SUMMARY---
Filename: psym-crashes/id:000544,sig:11,src:001515+007343,op:splice,rep:2
SHA1: 20de771b6086b1a3398115e4e2fc2841d0e50b64
Classification: PROBABLY_NOT_EXPLOITABLE
Hash: f580ca995a6ddc20b994fa723585917b.571d196ddb038b3eaa29ec225bc0ad52
Command: ./mp42aac psym-crashes/id:000544,sig:11,src:001515+007343,op:splice,rep:2 /tmp/out.aac
Faulting Frame:
AP4_DecoderConfigDescriptor::WriteFields(AP4_ByteStream&) @ 0x00005555555de356: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
Disassembly:
0x00005555555de342: test rbx,rbx
0x00005555555de345: je 0x5555555de365 <_ZN27AP4_DecoderConfigDescriptor11WriteFieldsER14AP4_ByteStream+133>
0x00005555555de347: nop WORD PTR [rax+rax*1+0x0]
0x00005555555de350: mov rdi,QWORD PTR [rbx]
0x00005555555de353: mov rsi,rbp
=> 0x00005555555de356: mov rax,QWORD PTR [rdi]
0x00005555555de359: call QWORD PTR [rax+0x10]
0x00005555555de35c: mov rbx,QWORD PTR [rbx+0x8]
0x00005555555de360: test rbx,rbx
0x00005555555de363: jne 0x5555555de350 <_ZN27AP4_DecoderConfigDescriptor11WriteFieldsER14AP4_ByteStream+112>
Stack Head (11 entries):
AP4_DecoderConfigDescript @ 0x00005555555de356: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_Expandable::Write(AP4 @ 0x00005555555e109d: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_DecoderConfigDescript @ 0x00005555555de35c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_Expandable::Write(AP4 @ 0x00005555555e109d: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_EsDescriptor::WriteFi @ 0x00005555555e06fc: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_Expandable::Write(AP4 @ 0x00005555555e109d: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_Atom::Clone() @ 0x00005555555c87e7: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_AvcSampleDescription: @ 0x00005555555b4eef: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_AvcSampleEntry::ToSam @ 0x00005555555b7b5f: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_StsdAtom::GetSampleDe @ 0x00005555555bbf0d: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
main @ 0x00005555555ab4d2: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
Registers:
rax=0x0000000000000000 rbx=0x000055555568e4e0 rcx=0x0000000000000000 rdx=0x0000000000000004
rsi=0x000055555568f5a0 rdi=0x0000000000000000 rbp=0x000055555568f5a0 rsp=0x00007fffffffd940
r8=0x000055555568f5d0 r9=0x000000000000007c r10=0x0000000000000000 r11=0x00007ffff7d93be0
r12=0x0000000000000000 r13=0x000055555568f5a0 r14=0x000055555568f540 r15=0x0000555555636d10
rip=0x00005555555de356 efl=0x0000000000010202 cs=0x0000000000000033 ss=0x000000000000002b
ds=0x0000000000000000 es=0x0000000000000000 fs=0x0000000000000000 gs=0x0000000000000000
Extra Data:
Description: Access violation near NULL on source operand
Short description: SourceAvNearNull (16/22)
Explanation: The target crashed on an access violation at an address matching the source operand of the current instruction. This likely indicates a read access violation, which may mean the application crashed on a simple NULL dereference to data structure that has no immediate effect on control of the processor.
---END SUMMARY---
```

## Information provided by address sanitizer:

## AddressSanitizer:DEADLYSIGNAL

```
==22201==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000061a6d8 bp 0x7ffdd0eee230 sp 0x7ffdd0eee170 T0)
==22201==The signal is caused by a READ memory access.
==22201==Hint: address points to the zero page.
#0 0x61a6d7 in AP4_DescriptorListWriter::Action(AP4_Descriptor*) const /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Descriptor.h:108:28
#1 0x6199fe in AP4_List<AP4_Descriptor>::Apply(AP4_List<AP4_Descriptor>::Item::Operator const&) const /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4List.h:353:12
#2 0x6199fe in AP4_DecoderConfigDescriptor::WriteFields(AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4DecoderConfigDescriptor.cpp:123
#3 0x622297 in AP4_Expandable::Write(AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Expandable.cpp:109:5
#4 0x6199fe in AP4_List<AP4_Descriptor>::Apply(AP4_List<AP4_Descriptor>::Item::Operator const&) const /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4List.h:353:12
#5 0x6199fe in AP4_DecoderConfigDescriptor::WriteFields(AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4DecoderConfigDescriptor.cpp:123
#6 0x622297 in AP4_Expandable::Write(AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Expandable.cpp:109:5
#7 0x620603 in AP4_List<AP4_Descriptor>::Apply(AP4_List<AP4_Descriptor>::Item::Operator const&) const /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4List.h:353:12
#8 0x620603 in AP4_EsDescriptor::WriteFields(AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4EsDescriptor.cpp:163
#9 0x622297 in AP4_Expandable::Write(AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Expandable.cpp:109:5
#10 0x5c8e54 in AP4_Atom::Clone() /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Atom.cpp:316:9
#11 0x58ddc6 in AP4_SampleDescription::AP4_SampleDescription(AP4_SampleDescription::Type, unsigned int, AP4_AtomParent*) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4SampleDescription.cpp:132:41
#12 0x58ddc6 in AP4_AvcSampleDescription::AP4_AvcSampleDescription(unsigned int, unsigned short, unsigned short, unsigned short, char const*, AP4_AtomParent*) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4SampleDescription.cpp:356
#13 0x59882a in AP4_AvcSampleEntry::ToSampleDescription() /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4SampleEntry.cpp:1022:16
#14 0x5a091e in AP4_StsdAtom::GetSampleDescription(unsigned int) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4StsdAtom.cpp:181:53
#15 0x5714b2 in main /home/natalie/Downloads/Bento4-master/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:268:39
#16 0x7f26839a31e2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x271e2)
#17 0x45c96d in _start (/home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac-asan+0x45c96d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Descriptor.h:108:28 in AP4_DescriptorListWriter::Action(AP4_Descriptor*) const
==22201==ABORTING
```

**barbibulle** self-assigned this on May 17, 2020

**barbibulle** added the **fuzzing** label on May 17, 2020

**natalie13m** commented on May 18, 2020 Author

Crash input:
https://github.com/natalie13m/crashes/blob/master/bento4-06c39d9/id:000544%2Csig:11%2Csrc:001515%2B007343%2Cop:splice%2Crep:2

Assignees

barbibulle

Labels

**fuzzing**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants