New issue

Jump to bottom

SEGV by a READ memory access (address points to the zero page) #511

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

Assignees

Labels fuzzing

natalie13m commented on May 16, 2020 • edited

Command:

```
./mp42aac @@ /tmp/out.aac
```

Information provided by address sanitizer

AddressSanitizer:DEADLYSIGNAL

```
==22974==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000068223f bp 0x7ffedd403b10 sp 0x7ffedd403970 T0)
==22974==The signal is caused by a READ memory access.
==22974==Hint: address points to the zero page.
#0 0x68223e in AP4_Stz2Atom::GetSampleSize(unsigned int, unsigned int&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Stz2Atom.cpp:197:23
#1 0x5d8790 in AP4_AtomSampleTable::GetSample(unsigned int, AP4_Sample&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomSampleTable.cpp
#2 0x5a32ce in AP4_Track::GetSample(unsigned int, AP4_Sample&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Track.cpp:435:43
#3 0x5a32ce in AP4_Track::ReadSample(unsigned int, AP4_Sample&, AP4_DataBuffer&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Track.cpp:469
#4 0x571a80 in WriteSamples(AP4_Track*, AP4_SampleDescription*, AP4_ByteStream*) /home/natalie/Downloads/Bento4-master/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:192:12
#5 0x571a80 in main /home/natalie/Downloads/Bento4-master/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:281
#6 0x7f865b36f1e2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x271e2)
#7 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/Ap4Stz2Atom.cpp:197:23 in AP4_Stz2Atom::GetSampleSize(unsigned int, unsigned int&)
==22974==ABORTING
```

Information provided by crashwalk:

```
---CRASH SUMMARY---
Filename: id:000397,sig:11,src:005796+004474,op:splice,rep:4
SHA1: 3765c3464711c3352df8daac331db1a61870e86a
Classification: PROBABLY_NOT_EXPLOITABLE
Hash: 07d82808978ec56bef294c76fd303f3b.07d82808978ec56bef294c76fd303f3b
Command: ./mp42aac psym-crashes/id:000397,sig:11,src:005796+004474,op:splice,rep:4 /tmp/out.aac
Faulting Frame:
AP4_Stz2Atom::GetSampleSize(unsigned int, unsigned int&) @ 0x00005555555f9b74: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
Disassembly:
0x00005555555f9b67: jb 0x5555555f9b80 <_ZN12AP4_Stz2Atom13GetSampleSizeEjRj+32>
0x00005555555f9b69: test esi,esi
0x00005555555f9b6b: je 0x5555555f9b80 <_ZN12AP4_Stz2Atom13GetSampleSizeEjRj+32>
0x00005555555f9b6d: mov rax,QWORD PTR [rdi+0x40]
0x00005555555f9b71: lea ecx,[rsi-0x1]
=> 0x00005555555f9b74: mov ecx,DWORD PTR [rax+rcx*4]
0x00005555555f9b77: xor eax,eax
0x00005555555f9b79: mov DWORD PTR [rdx],ecx
0x00005555555f9b7b: ret
0x00005555555f9b7c: nop DWORD PTR [rax+0x0]
Stack Head (4 entries):
AP4_Stz2Atom::GetSampleSi @ 0x00005555555f9b74: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_AtomSampleTable::GetS @ 0x00005555555ce999: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_Track::ReadSample(uns @ 0x00005555555bd910: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
main @ 0x00005555555ab76c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
Registers:
rax=0x0000000000000000 rbx=0x00005555556559c0 rcx=0x0000000000000000 rdx=0x00007fffffffdb04
rsi=0x0000000000000001 rdi=0x00005555556554a0 rbp=0x0000000000000001 rsp=0x00007fffffffdae8
r8=0x0000000000000000 r9=0x0000000000000000 r10=0x0000000000000000 r11=0x000000000000000a
r12=0x0000000000000000 r13=0x00007fffffffdb10 r14=0x00007fffffffdbf0 r15=0x0000000000000001
rip=0x00005555555f9b74 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---
```

barbibulle self-assigned this on May 17, 2020

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

natalie13m commented on May 18, 2020 Author

https://github.com/natalie13m/crashes/blob/master/bento4-06c39d9/id:000397%2Csig:11%2Csrc:005796%2B004474%2Cop:splice%2Crep:4

barbibulle closed this as completed in `c9f2c53` on May 21, 2020

barbibulle mentioned this issue on Jun 11, 2020

Bento4 mp4dash to encrypt Dolby Vision MP4 video with Playready does not play #517

Closed

Assignees

barbibulle

Labels

fuzzing

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants