

New issue

[Jump to bottom](#)

SEGV error #758

Open plcici opened this issue on Sep 17 · 0 comments

Assignees



Labels

fuzzing

plcici commented on Sep 17 • edited ▼

Hi there, I use my fuzzer for fuzzing the binary mp4decrypt, and this binary crashes with the following:

```
AddressSanitizer:DEADLYSIGNAL
=====
==24087==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x000000702ee8 bp
0x7ffcf40a75f0 sp 0x7ffcf40a73b0 T0)
==24087==The signal is caused by a READ memory access.
==24087==Hint: address points to the zero page.
#0 0x702ee8 in AP4_StszAtom::WriteFields(AP4_ByteStream&)
(/fuzztest/mp4decrypt/mp4decrypt+0x702ee8)
#1 0x82facf in AP4_AtomListWriter::Action(AP4_Atom*) const
(/fuzztest/mp4decrypt/mp4decrypt+0x82facf)
#2 0x4fc423 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/fuzztest/mp4decrypt/mp4decrypt+0x4fc423)
#3 0x82facf in AP4_AtomListWriter::Action(AP4_Atom*) const
(/fuzztest/mp4decrypt/mp4decrypt+0x82facf)
#4 0x4fc423 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/fuzztest/mp4decrypt/mp4decrypt+0x4fc423)
#5 0x82facf in AP4_AtomListWriter::Action(AP4_Atom*) const
(/fuzztest/mp4decrypt/mp4decrypt+0x82facf)
#6 0x4fc423 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/fuzztest/mp4decrypt/mp4decrypt+0x4fc423)
#7 0x82facf in AP4_AtomListWriter::Action(AP4_Atom*) const
(/fuzztest/mp4decrypt/mp4decrypt+0x82facf)
#8 0x4fc423 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/fuzztest/mp4decrypt/mp4decrypt+0x4fc423)
#9 0x82facf in AP4_AtomListWriter::Action(AP4_Atom*) const
(/fuzztest/mp4decrypt/mp4decrypt+0x82facf)
#10 0x4fc423 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/fuzztest/mp4decrypt/mp4decrypt+0x4fc423)
#11 0x82facf in AP4_AtomListWriter::Action(AP4_Atom*) const
```

```
(/fuzztest/mp4decrypt/mp4decrypt+0x82facf)
#12 0x62cea7 in AP4_Processor::Process(AP4_ByteStream&, AP4_ByteStream&, AP4_ByteStream*,
AP4_Processor::ProgressListener*, AP4_AtomFactory&) (/fuzztest/mp4decrypt/mp4decrypt+0x62cea7)
#13 0x412846 in main (/fuzztest/mp4decrypt/mp4decrypt+0x412846)
#14 0x7fcaa49f1c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
#15 0x407c99 in _start (/fuzztest/mp4decrypt/mp4decrypt+0x407c99)
```

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/fuzztest/mp4decrypt/mp4decrypt+0x702ee8) in
AP4_StszAtom::WriteFields(AP4_ByteStream&)
==24087==ABORTING

System Details

Test Machine: Ubuntu 18.04 (docker)
Project Name: mp4decrypt (Bento4-1.6.0-639)

Command


./mp4decrypt mp4decrypt.demo /dev/null

Poc

[mp4decrypt_Poc.zip](#)

Credit

Wanying Cao(NCNIPC of China)
Han Zheng (NCNIPC of China, [Hexhive](#))

  **barbibulle** self-assigned this on Sep 18

  **barbibulle** added the **fuzzing** label on Sep 18

Assignees

 **barbibulle**

Labels

fuzzing

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

