SEGV at AP4_StszAtom::GetSampleSize(unsigned int, unsigned int&) in binary mp42ts #757

Open plcici opened this issue on Sep 16 · 2 comments

plcici commented on Sep 16 • edited

Hi There,
I tested the binary mp42ts with my fuzzer, and a crash incurred, i.e., SEGV on an unknown address error. Here are the details:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==6287==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000007021ab bp
0x7fff9e86cb50 sp 0x7fff9e86c5f0 T0)
==6287==The signal is caused by a READ memory access.
==6287==Hint: address points to the zero page.
    #0 0x7021ab in AP4_StszAtom::GetSampleSize(unsigned int, unsigned int&)
(/fuzztest/mp42ts/mp42ts+0x7021ab)
    #1 0x5754fc in AP4_AtomSampleTable::GetSample(unsigned int, AP4_Sample&)
(/fuzztest/mp42ts/mp42ts+0x5754fc)
    #2 0x40d0cb in TrackSampleReader::ReadSample(AP4_Sample&, AP4_DataBuffer&)
(/fuzztest/mp42ts/mp42ts+0x40d0cb)
    #3 0x418342 in main (/fuzztest/mp42ts/mp42ts+0x418342)
    #4 0x7f9ae1a41c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #5 0x407c99 in _start (/fuzztest/mp42ts/mp42ts+0x407c99)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/fuzztest/mp42ts/mp42ts+0x7021ab) in
AP4_StszAtom::GetSampleSize(unsigned int, unsigned int&)
==6287==ABORTING
```

System Details

Test Machine: Ubuntu 18.04 (docker)
Project Name: mp42ts (Bento4-1.6.0-639)

Command

```
./mp42ts mp42ts.demo /dev/null
```

Poc

mp42ts_Poc.zip

Credit

Wanying Cao (NCNIPC of China)
Han Zheng (NCNIPC of China, Hexhive)

barbibulle commented on Sep 18 Contributor

This does not occur with the latest commit of the master branch. Could you double check?

plcici commented on Sep 19 Author

> This does not occur with the latest commit of the master branch. Could you double check?
> Sorry, we used the latest release (but not the latest commit) by mistake. Considering there are no reports and patch records corresponding to this bug, I suspect this bug might still exist. We could try to reproduce it in the latest commit version. Thanks for your time and reply.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants