New issue

Jump to bottom

Out of memory in AP4_CttsAtom::Create(unsigned int, AP4_ByteStream&) #755

Open yuhanghuang opened this issue on Sep 14 · 2 comments

yuhanghuang commented on Sep 14 • edited

summary

Hello, I use my fuzzer to fuzz binary mp4tag mp4split and mp42hevc, the three binary all crashede, and shows that allocator is out of memory trying to allocate 0xxxxxxx bytes. The version of Bento4 is the latest and the operation system is Ubuntu 18.04(docker). The following is the details.

Bug1

```
root@c511e4bf49bc:/mp42hevc/mp42hevc# ./mp42hevc seed.demo out.hevc
=================================================================
==92089==ERROR: AddressSanitizer: allocator is out of memory trying to allocate 0x54ba37b78 bytes
    #0 0xa1b020 in malloc /llvm/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x7fe65b2d6297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
    #2 0x6c1b9b in AP4_CttsAtom::Create(unsigned int, AP4_ByteStream&)
(/mp42hevc/mp42hevc/mp42hevc+0x6c1b9b)
    #3 0x5cf24c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/mp42hevc/mp42hevc/mp42hevc+0x5cf24c)
    #4 0x5dcbb6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/mp42hevc/mp42hevc/mp42hevc+0x5dcbb6)
    #5 0x6bd7a5 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/mp42hevc/mp42hevc/mp42hevc+0x6bd7a5)
    #6 0x6bc7f9 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/mp42hevc/mp42hevc/mp42hevc+0x6bc7f9)
    #7 0x5d5f65 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/mp42hevc/mp42hevc/mp42hevc+0x5d5f65)
    #8 0x5dcbb6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/mp42hevc/mp42hevc/mp42hevc+0x5dcbb6)
    #9 0x6bd7a5 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/mp42hevc/mp42hevc/mp42hevc+0x6bd7a5)
    #10 0x6bcf4a in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
```

```
AP4_ByteStream&, AP4_AtomFactory&) (/mp42hevc/mp42hevc/mp42hevc+0x6bcf4a)
    #11 0x5d5abc in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/mp42hevc/mp42hevc/mp42hevc+0x5d5abc)
    #12 0x5dcbb6 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/mp42hevc/mp42hevc/mp42hevc+0x5dcbb6)
    #13 0x6bd7a5 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/mp42hevc/mp42hevc/mp42hevc+0x6bd7a5)
    #14 0x6bfa61 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/mp42hevc/mp42hevc/mp42hevc+0x6bfa61)

==92089==HINT: if you don't care about these errors you may set allocator_may_return_null=1
SUMMARY: AddressSanitizer: out-of-memory /llvm/llvm-project/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145 in malloc
==92089==ABORTING
my test case:
```

Bug2

```
root@c511e4bf49bc:/mp42hevc/mp42hevc# /mp4box/mp4tag/mp4tag /mp4box/mp4tag/seed.demo
=================================================================
==843687==ERROR: AddressSanitizer: allocator is out of memory trying to allocate 0x3a35b4320 bytes
    #0 0xa38ee0 in malloc /llvm/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x7f9f81086297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
    #2 0x4ae28b in AP4_CttsAtom::Create(unsigned int, AP4_ByteStream&)
(/mp4box/mp4tag/mp4tag+0x4ae28b)
    #3 0x45f0fc in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/mp4box/mp4tag/mp4tag+0x45f0fc)
    #4 0x46ca96 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/mp4box/mp4tag/mp4tag+0x46ca96)
    #5 0x4a9e92 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/mp4box/mp4tag/mp4tag+0x4a9e92)
    #6 0x4ac151 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/mp4box/mp4tag/mp4tag+0x4ac151)

==843687==HINT: if you don't care about these errors you may set allocator_may_return_null=1
SUMMARY: AddressSanitizer: out-of-memory /llvm/llvm-project/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145 in malloc
==843687==ABORTING
```

Bug3

```
root@c511e4bf49bc:/mp4split/mp4split# ./mp4split
FishFuzz/crashes/id:000025,sig:06,src:000215,op:flip1,pos:31468,26038495
=================================================================
==3151765==ERROR: AddressSanitizer: allocator is out of memory trying to allocate 0x400000068
```

```
bytes
    #0 0xa19d40 in malloc /llvm/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x7f8d59cb9297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
    #2 0x48fc9b in AP4_CttsAtom::Create(unsigned int, AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x48fc9b)
    #3 0x440aec in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/mp4split/mp4split/mp4split+0x440aec)
    #4 0x44e46b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/mp4split/mp4split/mp4split+0x44e46b)
    #5 0x48b8a5 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/mp4split/mp4split/mp4split+0x48b8a5)
    #6 0x48b04a in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/mp4split/mp4split/mp4split+0x48b04a)
    #7 0x44735c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/mp4split/mp4split/mp4split+0x44735c)
    #8 0x44e46b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/mp4split/mp4split/mp4split+0x44e46b)
    #9 0x48b8a5 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/mp4split/mp4split/mp4split+0x48b8a5)
    #10 0x48b04a in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/mp4split/mp4split/mp4split+0x48b04a)
    #11 0x44735c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/mp4split/mp4split/mp4split+0x44735c)
    #12 0x44e46b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/mp4split/mp4split/mp4split+0x44e46b)
    #13 0x48b8a5 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/mp4split/mp4split/mp4split+0x48b8a5)
    #14 0x48b04a in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/mp4split/mp4split/mp4split+0x48b04a)
    #15 0x44735c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/mp4split/mp4split/mp4split+0x44735c)
    #16 0x44e46b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/mp4split/mp4split/mp4split+0x44e46b)
    #17 0x48b8a5 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/mp4split/mp4split/mp4split+0x48b8a5)
    #18 0x48db61 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/mp4split/mp4split/mp4split+0x48db61)

==3151765==HINT: if you don't care about these errors you may set allocator_may_return_null=1
SUMMARY: AddressSanitizer: out-of-memory /llvm/llvm-project/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145 in malloc
==3151765==ABORTING
```

POC

MP42hevc_crash.zip
MP4tag_crash.zip
mp4split_crash.zip

Credit

Yuhang Huang (NCNIPC of China)
Han Zheng (NCNIPC of China, Hexhive)

Thank you for your time!

barbibulle commented on Sep 18 Contributor

I am not able to replicate the issue with the latest commit on the master branch. Could you try with that version?

yuhanghuang commented on Sep 19 Author

> I am not able to replicate the issue with the latest commit on the master branch. Could you try with that version?

Sorry,
It is my problem. I have use the latest commit 5b7cc25 and commit 5b7cc25 to test, finding the problem indeed has been fixed. I use the v1.6.0-639 release version to test, and the use clang/clang++ 12.0.1 to compile the project in Ubuntu 18.04 operation system . While in the latest commit version,the problem has been fixed. Since the similar issues have not been comitted, I am trying to do more tests to make the issue can be replicated in the latest commit version.
Thanks for your reply!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants