

New issue

[Jump to bottom](#)

[BUG] Heap buffer overflow in AP4_HvccAtom, mp4tag #677

🔓 Open

kdsjZh opened this issue on Mar 13 · 2 comments

Assignees



Labels

fuzzing

kdsjZh commented on Mar 13 • edited ▾

brief description

There is a buffer overflow in AP4_HvccAtom, can be triggered via mp4tag + ASan.

To reproduce

```
mkdir build && pushd build
CC=clang CFLAGS="-fsanitize=address" CXX=clang CXXFLAGS="-fsanitize=address" cmake .. && make -j$(nproc)
./mp4tag --list-symbols --list-keys --show-tags $POC
```

output

```
=====
==2542087==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6030000003e6 at pc
0x0000004cfa61 bp 0x7ffffec70440 sp 0x7ffffec70430
READ of size 1 at 0x6030000003e6 thread T0
    #0 0x4cfa60 in AP4_HvccAtom::AP4_HvccAtom(unsigned int, unsigned char const*)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x4cfa60)
    #1 0x4cc7e5 in AP4_HvccAtom::Create(unsigned int, AP4_ByteStream&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x4cc7e5)
    #2 0x446dc2 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x446dc2)
    #3 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)
```

#4 0x47eccf in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47eccf)

#5 0x5779a8 in AP4_SampleEntry::Read(AP4_ByteStream&, AP4_AtomFactory&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x5779a8)

#6 0x58e0bb in AP4_VisualSampleEntry::AP4_VisualSampleEntry(unsigned int, unsigned int, AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x58e0bb)

#7 0x58f042 in AP4_AvcSampleEntry::AP4_AvcSampleEntry(unsigned int, unsigned int, AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x58f042)

#8 0x44241c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x44241c)

#9 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)

#10 0x5bbbb7 in AP4_StsdAtom::AP4_StsdAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x5bbbb7)

#11 0x5bafbd in AP4_StsdAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x5bafbd)

#12 0x445b0e in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x445b0e)

#13 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)

#14 0x47eccf in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47eccf)

#15 0x47f58d in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47f58d)

#16 0x47df78 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47df78)

#17 0x44c562 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x44c562)

#18 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)

#19 0x47eccf in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47eccf)

#20 0x47f58d in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47f58d)

#21 0x47df78 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47df78)

#22 0x44c562 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x44c562)

#23 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)

#24 0x47eccf in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47eccf)

#25 0x47f58d in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47f58d)

#26 0x47df78 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47df78)

#27 0x44c562 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x44c562)

#28 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)

#29 0x47eccf in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47eccf)

#30 0x47f58d in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47f58d)

#31 0x5f6668 in AP4_TrakAtom::AP4_TrakAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x5f6668)

```

#32 0x7a7726 in AP4_TrakAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x7a7726)
#33 0x444cfd in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x444cfd)
#34 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)
#35 0x47eccf in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47eccf)
#36 0x47f58d in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47f58d)
#37 0x50703e in AP4_MoovAtom::AP4_MoovAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x50703e)
#38 0x7a75e6 in AP4_MoovAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x7a75e6)
#39 0x4446b7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x4446b7)
#40 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)
#41 0x44e49a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x44e49a)
#42 0x4baaee in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x4baaee)
#43 0x4bc068 in AP4_File::AP4_File(AP4_ByteStream&, bool)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x4bc068)
#44 0x4090ab in main (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x4090ab)
#45 0x7f9977c8b0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
#46 0x4078bd in _start (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x4078bd)

```

0x6030000003e6 is located 0 bytes to the right of 22-byte region [0x6030000003d0,0x6030000003e6) allocated by thread T0 here:

```

#0 0x907b17 in operator new[](unsigned long)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x907b17)
#1 0x4a2314 in AP4_DataBuffer::AP4_DataBuffer(unsigned int)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x4a2314)
#2 0x4cc5dc in AP4_HvccAtom::Create(unsigned int, AP4_ByteStream&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x4cc5dc)
#3 0x446dc2 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x446dc2)
#4 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)
#5 0x47eccf in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47eccf)
#6 0x5779a8 in AP4_SampleEntry::Read(AP4_ByteStream&, AP4_AtomFactory&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x5779a8)
#7 0x58e0bb in AP4_VisualSampleEntry::AP4_VisualSampleEntry(unsigned int, unsigned int,
AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x58e0bb)
#8 0x58f042 in AP4_AvcSampleEntry::AP4_AvcSampleEntry(unsigned int, unsigned int,
AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x58f042)
#9 0x44241c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x44241c)
#10 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)
#11 0x5bbbb7 in AP4_StsdAtom::AP4_StsdAtom(unsigned int, unsigned char, unsigned int,
AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x5bbbb7)
#12 0x5bafbd in AP4_StsdAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x5bafbd)

```

```

#13 0x445b0e in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x445b0e)
#14 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)
#15 0x47eccf in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47eccf)
#16 0x47f58d in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47f58d)
#17 0x47df78 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47df78)
#18 0x44c562 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x44c562)
#19 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)
#20 0x47eccf in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47eccf)
#21 0x47f58d in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47f58d)
#22 0x47df78 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47df78)
#23 0x44c562 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x44c562)
#24 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)
#25 0x47eccf in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47eccf)
#26 0x47f58d in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47f58d)
#27 0x47df78 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x47df78)
#28 0x44c562 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x44c562)
#29 0x45123b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x45123b)

```

SUMMARY: AddressSanitizer: heap-buffer-overflow

(/home/hzheng/workspace/fuzz/mp4tag/mp4tag+0x4cfa60) in AP4_HvccAtom::AP4_HvccAtom(unsigned int, unsigned char const*)

Shadow bytes around the buggy address:

```

0x0c067fff8020: 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa
0x0c067fff8030: fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00
0x0c067fff8040: 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
0x0c067fff8050: fd fd fd fa fa fa 00 00 04 fa fa fa 00 00 00 fa
0x0c067fff8060: fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00
=>0x0c067fff8070: 00 fa fa fa 00 00 00 fa fa fa 00 00[06]fa fa fa
0x0c067fff8080: 00 00 06 fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c067fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

```

Shadow byte legend (one shadow byte represents 8 application bytes):

```

Addressable:          00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:    fa
Freed heap region:    fd
Stack left redzone:   f1

```

```
Stack mid redzone:      f2
Stack right redzone:    f3
Stack after return:     f5
Stack use after scope:  f8
Global redzone:         f9
Global init order:      f6
Poisoned by user:       f7
Container overflow:     fc
Array cookie:           ac
Intra object redzone:   bb
ASan internal:          fe
Left alloca redzone:    ca
Right alloca redzone:    cb
Shadow gap:             cc
==2542087==ABORTING
```

System


Ubuntu 20.04
clang 12.0.1
Bento4 latest commit [46dd88c](#)

Credit

Han Zheng ([NCNIPC of China](#), [Hexhive](#))
Yin Li, Xiaotong Jiao (NCNIPC of China)

POC

[poc.zip](#)

  **barbibulle** self-assigned this on May 1

barbibulle commented on May 1

Contributor

The issue doesn't seem to happen with the latest commit on the main branch. Can you confirm?

  **barbibulle** added the **fuzzing** label on May 1

kdsjZh commented on May 2

Author


Hello, this issue seems still happens in latest commit. my test environment: Ubuntu 20.04.3 LTS, gcc 9.3.0.

  **Yhcrown** mentioned this issue on Aug 1

Heap-Buffer-Overflow with ASAN in mp4info (AP4_HvccAtom) #736

 **Open**

Assignees

 **barbibulle**

Labels

fuzzing

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

