

New issue

[Jump to bottom](#)

## Heap buffer overflow in AP4\_StdCFileByteStream::ReadPartial #510



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:

```
=====
==22589==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000000b1 at pc 0x0000004e57a0 bp 0x7ffddd2a7340 sp 0x7ffddd2a6af0
WRITE of size 439 at 0x6020000000b1 thread T0
#0 0x4e579f in __interceptor_fread.part.52 /home/natalie/Research/LLVM/src/llvm-8.0.1.src/projects/compiler-rt/lib/asan/_/sanitizer_common/sanitizer_common_interceptors.inc:1001:16
#1 0x5c40ab in AP4_StdCFileByteStream::ReadPartial(void*, unsigned int, unsigned int&) /home/natalie/Downloads/Bento4-master/Source/C++/System/StdC/AP4StdCFileByteStream.cpp:250:14
#2 0x57260a in AP4_ByteStream::Read(void*, unsigned int) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ByteStream.cpp:54:29
#3 0x662a82 in AP4_RtpAtom::AP4_RtpAtom(unsigned int, AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4RtpAtom.cpp:50:16
#4 0x5d40a7 in AP4_RtpAtom::Create(unsigned int, AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4RtpAtom.h:53:20
#5 0x5d40a7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:669
#6 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#7 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:194:12
#8 0x60d6ee in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:139:5
#9 0x60d6ee in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:88
#10 0x5d42b2 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:796:20
#11 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#12 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:194:12
#13 0x60d6ee in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:139:5
#14 0x60d6ee in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:88
#15 0x5d42b2 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:796:20
#16 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#17 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:194:12
#18 0x60e126 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:139:5
#19 0x5a3e4b in AP4_TrakAtom::AP4_TrakAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4TrakAtom.cpp:165:5
#20 0x5d37f8 in AP4_TrakAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4TrakAtom.h:58:20
#21 0x5d37f8 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:399
#22 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#23 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:194:12
#24 0x60e126 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4ContainerAtom.cpp:139:5
#25 0x57ccce in AP4_MoovAtom::AP4_MoovAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4MoovAtom.cpp:79:5
#26 0x5d4251 in AP4_MoovAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4MoovAtom.h:56:20
#27 0x5d4251 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:379
#28 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:233:14
#29 0x5d21eb in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4AtomFactory.cpp:153:12
#30 0x57920e in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4File.cpp:104:12
#31 0x5797bb in AP4_File::AP4_File(AP4_ByteStream&, bool) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4File.cpp:78:5
#32 0x571465 in main /home/natalie/Downloads/Bento4-master/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:250:22
#33 0x7fb0adb691e2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x271e2)
#34 0x45c96d in _start (/home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac-asan+0x45c96d)

0x6020000000b1 is located 0 bytes to the right of 1-byte region [0x6020000000b0,0x6020000000b1)
allocated by thread T0 here:
#0 0x56de20 in operator new[](unsigned long) /home/natalie/Research/LLVM/src/llvm-8.0.1.src/projects/compiler-rt/lib/asan/asan_new_delete.cc:109:3
#1 0x662a72 in AP4_RtpAtom::AP4_RtpAtom(unsigned int, AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/AP4RtpAtom.cpp:49:21
```

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/natalie/Research/LLVM/src/llvm-8.0.1.src/projects/compiler-rt/lib/asan/./sanitizer\_common/sanitizer\_common\_interceptors.inc:1001:16 in \_\_interceptor\_fread.part.52

Shadow bytes around the buggy address:

0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x0c047fff8000: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00  
=>0x0c047fff8010: fa fa 04 fa fa fa[01]fa fa fa fa fa fa fa fa  
0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa  
0x0c047fff8060: 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  
==22589==ABORTING

## Information provided by crashwalk:

---CRASH SUMMARY---

Filename: id:000346,sig:06,src:005414,op:ext\_AO,pos:773

SHA1: 47de1f27633138a72eb87e0b9183a6a434bc6a71

Classification: EXPLOITABLE

Hash: 2bffe3e28b7d836de8df2bd02ca37d2b.8940a281b43ef80c9adc7f441d8810f4

Command: ./mp42aac psym-crashes/id:000346,sig:06,src:005414,op:ext\_AO,pos:773 /tmp/out.aac

Faulting Frame:

operator new(unsigned long) @ 0x00007ffff7e5f1d9: in /usr/lib/x86\_64-linux-gnu/libstdc++.so.6.0.28

Disassembly:

0x00007ffff7bef3da: xor edx,edx

0x00007ffff7bef3dc: mov rsi,r9

0x00007ffff7bef3df: mov edi,0x2

0x00007ffff7bef3e4: mov eax,0xe

0x00007ffff7bef3e9: syscall

=> 0x00007ffff7bef3eb: mov rax,QWORD PTR [rsp+0x108]

0x00007ffff7bef3f3: xor rax,QWORD PTR fs:0x28

0x00007ffff7bef3fc: jne 0x7ffff7bef424 < \_GI\_raise+260>

0x00007ffff7bef3fe: mov eax,r8d

0x00007ffff7bef401: add rsp,0x118

Stack Head (32 entries):

\_\_GI\_raise @ 0x00007ffff7bef3eb: in (BL)

\_\_GI\_abort @ 0x00007ffff7bce899: in (BL)

\_\_libc\_message @ 0x00007ffff7c3938e: in (BL)

malloc\_printerr @ 0x00007ffff7c414dc: in (BL)

\_int\_malloc @ 0x00007ffff7c4488a: in (BL)

\_\_GI\_\_libc\_malloc @ 0x00007ffff7c46304: in (BL)

operator @ 0x00007ffff7e5f1d9: in /usr/lib/x86\_64-linux-gnu/libstdc++.so.6.0.28

AP4\_String::operator=(cha @ 0x000055555555bbc77: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4\_RtpAtom::AP4\_RtpAtom( @ 0x000055555555f3fee: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4\_AtomFactory::CreateAt @ 0x000055555555ccadd: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4\_AtomFactory::CreateAt @ 0x000055555555cdb9c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4\_ContainerAtom::ReadCh @ 0x000055555555db882: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4\_ContainerAtom::Create @ 0x000055555555dbbfd: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4\_AtomFactory::CreateAt @ 0x000055555555cb892: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4\_AtomFactory::CreateAt @ 0x000055555555cdb9c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

AP4\_ContainerAtom::ReadCh @ 0x000055555555db882: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac

Registers:

rax=0x0000000000000000 rbx=0x00007ffff7a59100 rcx=0x00007ffff7bef3eb rdx=0x0000000000000000

rsi=0x00007ffff7fce40 rdi=0x0000000000000000 rbp=0x00007ffff7d190 rsp=0x00007ffff7fce40

r8=0x0000000000000000 r9=0x00007ffff7fce40 r10=0x0000000000000008 r11=0x00000000000000246

r12=0x00007ffff7db0 r13=0x0000000000000010 r14=0x00007ffff7fb000 r15=0x00000000000000002

rip=0x00007ffff7bef3eb efl=0x00000000000000246 cs=0x0000000000000033 ss=0x0000000000000002b

ds=0x0000000000000000 es=0x0000000000000000 fs=0x0000000000000000 gs=0x0000000000000000

Extra Data:


Description: Heap error

Short description: HeapError (10/22)

Explanation: The target's backtrace indicates that libc has detected a heap error or that the target was executing a heap function when it stopped. This could be due to heap corruption, passing a bad pointer to a heap function such as free(), etc. Since heap errors might include buffer overflows, use-after-free situations, etc. they are generally considered exploitable.

---END SUMMARY---



 **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:000346%2Csig:06%2Csrc:005414%2Cop:ext\\_AO%2Cpos:773](https://github.com/natalie13m/crashes/blob/master/bento4-06c39d9/id:000346%2Csig:06%2Csrc:005414%2Cop:ext_AO%2Cpos:773)

 **Shadowblad3** mentioned this issue on Nov 11

Heap overflow in mp4info, ReadPartial, Ap4StdCFileByteStream.cpp:341 #812

 Open

Assignees

 **barbibulle**

Labels

**fuzzing**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

