New issue

Jump to bottom

SEGV on unknown address by a WRITE memory access in AP4_NullTerminatedStringAtom::AP4_NullTerminatedStringAtom(unsigned int, unsigned long long, AP4_ByteStream&) #508

Closed **natalie13m** opened this issue on May 16, 2020 · 1 comment

Assignees

Labels **fuzzing**

natalie13m commented on May 16, 2020 • edited

I found a crash by running "./mp42aac @@ /tmp/out.aac".
The crash is identified as "EXPLOITABLE" by crashwalk.

Information provided by crashwalk (!exploitable)

```
---CRASH SUMMARY---
Filename: id:000436,sig:11,src:005777,op:ext_AO,pos:697
SHA1: 6e5f8913397067951eb2e963701fd605b3bc168b
Classification: EXPLOITABLE
Hash: 7606cf035283a6a1bf64fe4bdc424dfb.c7ad0413c824b07ed97b196265be5bd9
Command: ./mp42aac psym-crashes/id:000436,sig:11,src:005777,op:ext_AO,pos:697 /tmp/out.aac
Faulting Frame:
AP4_NullTerminatedStringAtom::AP4_NullTerminatedStringAtom(unsigned int, unsigned long long, AP4_ByteStream&) @ 0x00005555555cac74: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
Disassembly:
0x00005555555cac63: mov r12,rax
0x00005555555cac66: call 0x5555555ac890 <_ZN14AP4_ByteStream4ReadEPvj>
0x00005555555cac6b: lea eax,[rbx-0x9]
0x00005555555cac6e: mov rsi,r12
0x00005555555cac71: mov rdi,rbp
=> 0x00005555555cac74: mov BYTE PTR [r12+rax*1],0x0
0x00005555555cac79: call 0x5555555bbc30 <_ZN10AP4_StringaSEPKc>
0x00005555555cac7e: pop rbx
0x00005555555cac7f: pop rbp
0x00005555555cac80: pop r12
Stack Head (20 entries):
AP4_NullTerminatedStringA @ 0x00005555555cac74: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_AtomFactory::CreateAt @ 0x00005555555cbac2: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_AtomFactory::CreateAt @ 0x00005555555cdb9c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_ContainerAtom::ReadCh @ 0x00005555555db882: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_ContainerAtom::Create @ 0x00005555555dbbfd: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_AtomFactory::CreateAt @ 0x00005555555cb892: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_AtomFactory::CreateAt @ 0x00005555555cdb9c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_ContainerAtom::ReadCh @ 0x00005555555db882: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_ContainerAtom::AP4_Co @ 0x00005555555db999: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_TrakAtom::AP4_TrakAto @ 0x00005555555bdef3: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_AtomFactory::CreateAt @ 0x00005555555cbf9c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_AtomFactory::CreateAt @ 0x00005555555cdb9c: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_ContainerAtom::ReadCh @ 0x00005555555db882: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_ContainerAtom::AP4_Co @ 0x00005555555db999: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_MoovAtom::AP4_MoovAto @ 0x00005555555aee5a: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
AP4_AtomFactory::CreateAt @ 0x00005555555cc87a: in /home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac
Registers:
rax=0x00000000ffffffff rbx=0x0000000000000008 rcx=0x0000555555654fe0 rdx=0x0000000000000000
rsi=0x0000555555654fd0 rdi=0x0000555555654fb8 rbp=0x0000555555654fb8 rsp=0x00007fffffffd470
r8=0x0000555555654fd0 r9=0x00007fffffffd598 r10=0x0000000000000008 r11=0x00007ffff7d93be0
r12=0x0000555555654fd0 r13=0x00005555556535a0 r14=0x0000000000000000 r15=0x00005555556535a0
rip=0x00005555555cac74 efl=0x0000000000010206 cs=0x0000000000000033 ss=0x000000000000002b
ds=0x0000000000000000 es=0x0000000000000000 fs=0x0000000000000000 gs=0x0000000000000000
Extra Data:
Description: Access violation on destination operand
Short description: DestAv (8/22)
Explanation: The target crashed on an access violation at an address matching the destination operand of the instruction. This likely indicates a write access violation, which means the attacker may control the write address and/or value.
---END SUMMARY---
```

Information provided by address sanitizer

```
=================================================================
==21893==ERROR: AddressSanitizer: SEGV on unknown address 0x6021000000cf (pc 0x0000005ca6ca bp 0x7ffdfe80f7d0 sp 0x7ffdfe80f6b0 T0)
==21893==The signal is caused by a WRITE memory access.
#0 0x5ca6c9 in AP4_NullTerminatedStringAtom::AP4_NullTerminatedStringAtom(unsigned int, unsigned long long, AP4_ByteStream&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Atom.cpp:474:21
#1 0x5d46e8 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:550:24
#2 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:233:14
#3 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4ContainerAtom.cpp:194:12
#4 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
#5 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
#6 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
#7 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:233:14
#8 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4ContainerAtom.cpp:194:12
#9 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
#10 0x5a3e4b in AP4_TrakAtom::AP4_TrakAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4TrakAtom.cpp:165:5
#11 0x5d37f8 in AP4_TrakAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4TrakAtom.h:58:20
#12 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
#13 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:233:14
#14 0x60e44b in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4ContainerAtom.cpp:194:12
#15 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
#16 0x57ccec in AP4_MoovAtom::AP4_MoovAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4MoovAtom.cpp:79:5
#17 0x5d4251 in AP4_MoovAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4MoovAtom.h:56:20
#18 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
#19 0x5d2922 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:233:14
#20 0x5d21eb in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4AtomFactory.cpp:153:12
#21 0x57920e in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4File.cpp:104:12
#22 0x5797bb in AP4_File::AP4_File(AP4_ByteStream&, bool) /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4File.cpp:78:5
#23 0x571465 in main /home/natalie/Downloads/Bento4-master/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:250:22
#24 0x7f2bab9ae1e2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x271e2)
#25 0x45c96d in _start (/home/natalie/Desktop/research/Bug/bento4-06c39d9/mp42aac-asan+0x45c96d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/natalie/Downloads/Bento4-master/Source/C++/Core/Ap4Atom.cpp:474:21 in AP4_NullTerminatedStringAtom::AP4_NullTerminatedStringAtom(unsigned int, unsigned long long, AP4_ByteStream&)
==21893==ABORTING
```

barbibulle self-assigned this on May 17, 2020

barbibulle added the **fuzzing** label on May 17, 2020

natalie13m commented on May 18, 2020 • edited ▾ 	Author

Crash file:
https://github.com/natalie13m/crashes/blob/master/bento4-06c39d9/id:000436%2Csig:11%2Csrc:005777%2Cop:ext_AO%2Cpos:697

barbibulle closed this as completed in `13a6e92` on May 21, 2020

Assignees

barbibulle

Labels

fuzzing

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants