

Description of problem:

Dos crash in AP4_CttsAtom::AP4_CttsAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&) /Bento4-SRC-1-5-1-622/Source/C++/Core/Ap4CttsAtom.cpp:80

Version-Release number of selected component (if applicable):

1.5.1.0

How reproducible:

./mp2aac POC /dev/null

Poc file: <https://drive.google.com/open?id=1SPvacl6vscc77wkptHMIais2ToIWM2DQ>

==98478==ERROR: AddressSanitizer failed to allocate 0xf8002000 (4160757760) bytes of LargeMmapAllocator (errno: 12)

==98478==Process memory map follows:

```
0x0000000400000-0x0000000776000
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/mp42aac
0x0000000975000-0x0000000976000
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/mp42aac
0x0000000976000-0x0000000b05000
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/mp42aac
0x0000000b05000-0x0000000b06000
0x000007fff7000-0x000008fff7000
0x000008fff7000-0x02008fff7000
0x02008fff7000-0x10007fff8000
0x6000000000000-0x6020000000000
0x6020000000000-0x602000010000
0x602000010000-0x6030000000000
0x6030000000000-0x603000010000
0x603000010000-0x6040000000000
0x6040000000000-0x604000010000
0x604000010000-0x6070000000000
0x6070000000000-0x607000010000
0x607000010000-0x6080000000000
0x6080000000000-0x608000010000
0x608000010000-0x6160000000000
0x6160000000000-0x616000020000
0x616000020000-0x6190000000000
0x6190000000000-0x619000020000
0x619000020000-0x6210000000000
```

0x621000000000-0x621000020000
0x621000020000-0x624000000000
0x624000000000-0x624000020000
0x624000020000-0x631000000000
0x631000000000-0x631000030000
0x631000030000-0x640000000000
0x640000000000-0x640000030000
0x7f9208efe000-0x7f9301000000
0x7f9301100000-0x7f9301200000
0x7f9301230000-0x7f9303582000
0x7f9303582000-0x7f930368a000 /lib/x86_64-linux-gnu/libm-2.23.so
0x7f930368a000-0x7f9303889000 /lib/x86_64-linux-gnu/libm-2.23.so
0x7f9303889000-0x7f930388a000 /lib/x86_64-linux-gnu/libm-2.23.so
0x7f930388a000-0x7f930388b000 /lib/x86_64-linux-gnu/libm-2.23.so
0x7f930388b000-0x7f930388e000 /lib/x86_64-linux-gnu/libdl-2.23.so
0x7f930388e000-0x7f9303a8d000 /lib/x86_64-linux-gnu/libdl-2.23.so
0x7f9303a8d000-0x7f9303a8e000 /lib/x86_64-linux-gnu/libdl-2.23.so
0x7f9303a8e000-0x7f9303a8f000 /lib/x86_64-linux-gnu/libdl-2.23.so
0x7f9303a8f000-0x7f9303aa7000 /lib/x86_64-linux-gnu/libpthread-2.23.so
0x7f9303aa7000-0x7f9303ca6000 /lib/x86_64-linux-gnu/libpthread-2.23.so
0x7f9303ca6000-0x7f9303ca7000 /lib/x86_64-linux-gnu/libpthread-2.23.so
0x7f9303ca7000-0x7f9303ca8000 /lib/x86_64-linux-gnu/libpthread-2.23.so
0x7f9303ca8000-0x7f9303cac000
0x7f9303cac000-0x7f9303e6c000 /lib/x86_64-linux-gnu/libc-2.23.so
0x7f9303e6c000-0x7f930406c000 /lib/x86_64-linux-gnu/libc-2.23.so
0x7f930406c000-0x7f9304070000 /lib/x86_64-linux-gnu/libc-2.23.so
0x7f9304070000-0x7f9304072000 /lib/x86_64-linux-gnu/libc-2.23.so
0x7f9304072000-0x7f9304076000
0x7f9304076000-0x7f930408c000 /lib/x86_64-linux-gnu/libgcc_s.so.1
0x7f930408c000-0x7f930428b000 /lib/x86_64-linux-gnu/libgcc_s.so.1
0x7f930428b000-0x7f930428c000 /lib/x86_64-linux-gnu/libgcc_s.so.1
0x7f930428c000-0x7f93043fe000 /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21
0x7f93043fe000-0x7f93045fe000 /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21
0x7f93045fe000-0x7f9304608000 /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21
0x7f9304608000-0x7f930460a000 /usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.21
0x7f930460a000-0x7f930460e000
0x7f930460e000-0x7f9304702000 /usr/lib/x86_64-linux-gnu/libasan.so.2.0.0
0x7f9304702000-0x7f9304902000 /usr/lib/x86_64-linux-gnu/libasan.so.2.0.0
0x7f9304902000-0x7f9304905000 /usr/lib/x86_64-linux-gnu/libasan.so.2.0.0
0x7f9304905000-0x7f9304906000 /usr/lib/x86_64-linux-gnu/libasan.so.2.0.0
0x7f9304906000-0x7f930557b000
0x7f930557b000-0x7f93055a1000 /lib/x86_64-linux-gnu/ld-2.23.so
0x7f93055a1000-0x7f9305768000

```

0x7f9305768000-0x7f93057a0000
0x7f93057a0000-0x7f93057a1000    /lib/x86_64-linux-gnu/ld-2.23.so
0x7f93057a1000-0x7f93057a2000    /lib/x86_64-linux-gnu/ld-2.23.so
0x7f93057a2000-0x7f93057a3000
0x7ffc90a4e000-0x7ffc90a6f000    [stack]
0x7ffc90b2f000-0x7ffc90b32000    [vvar]
0x7ffc90b32000-0x7ffc90b34000    [vdso]
0xffffffff600000-0xffffffff601000 [vsyscall]
==98478==End of process memory map.
==98478==AddressSanitizer CHECK failed:
../../../../src/libsanitizer/sanitizer_common/sanitizer_posix.cc:121 ("unable to mmap" && 0) !=
(0)" (0x0, 0x0)
#0 0x7f93046ae631 (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xa0631)
#1 0x7f93046b35e3 in __sanitizer::CheckFailed(char const*, int, char const*, unsigned long
long, unsigned long long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xa55e3)
#2 0x7f93046bb611 (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xad611)
#3 0x7f9304630c0c (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x22c0c)
#4 0x7f93046a767e in operator new[](unsigned long)
(/usr/lib/x86_64-linux-gnu/libasan.so.2+0x9967e)
#5 0x4cc09c in AP4_CttsAtom::AP4_CttsAtom(unsigned int, unsigned char, unsigned int,
AP4_ByteStream&)
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/Source/C++/Core/AP4CttsAtom.cpp:80
#6 0x4cbd1d in AP4_CttsAtom::Create(unsigned int, AP4_ByteStream&)
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/Source/C++/Core/AP4CttsAtom.cpp:52
#7 0x489705 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned
int, unsigned int, unsigned long long, AP4_Atom*&)
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/Source/C++/Core/AP4AtomFactory.cpp
:457
#8 0x487c62 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned
long long&, AP4_Atom*&)
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/Source/C++/Core/AP4AtomFactory.cpp
:220
#9 0x4875b7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&,
AP4_Atom*&)
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/Source/C++/Core/AP4AtomFactory.cpp
:150
#10 0x455fe1 in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool)
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/Source/C++/Core/AP4File.cpp:104
#11 0x455c50 in AP4_File::AP4_File(AP4_ByteStream&, bool)
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/Source/C++/Core/AP4File.cpp:78
#12 0x451590 in main
/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/Source/C++/Apps/Mp42Aac/Mp42Aac.
cpp:250

```

#13 0x7f9303ccc82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#14 0x4505c8 in _start
(/home/puppet/test_object_video/Bento4-SRC-1-5-1-622/mp42aac+0x4505c8)

Actual results:

crash

Expected results:

crash

Additional info:

This vulnerability is detected by NESA Lab(nesa.zju.edu.cn), with our custom seed generate system, SmartSeed. Please contact puppet@zju.edu.cn and albertzjf@163.com if you need more info about the team, the tool or the vulnerability.