New issue

Jump to bottom

there are some bugs in Bento4 #775

Open **yuhanghuang** opened this issue on Sep 24 · 0 comments

yuhanghuang commented on Sep 24 • edited

Hello, I use fuzer to test binary acc2mp4, and found some carshes, which can result binary mp4split crash too. Here are the details.

Bug1

```
root@d5f4647d38bd:/aac2mp4/aac2mp4# /Bento4/build/aac2mp4 crash1 /dev/null
AAC frame [000000]: size = -7, 96000 kHz, 0 ch
=================================================================
==813117==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62d000008400 at pc
0x0000004ad912 bp 0x7ffe2c57b390 sp 0x7ffe2c57ab40
READ of size 4294967287 at 0x62d000008400 thread T0
    #0 0x4ad911 in __asan_memcpy /llvm-project/compiler-
rt/lib/asan/asan_interceptors_memintrinsics.cpp:22
    #1 0x4facae in AP4_BitStream::ReadBytes(unsigned char*, unsigned int)
/Bento4/Source/C++/Codecs/Ap4BitStream.cpp:192:10
    #2 0x4f8485 in main /Bento4/Source/C++/Apps/Aac2Mp4/Aac2Mp4.cpp:142:29
    #3 0x7fec98881c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #4 0x41c349 in _start (/Bento4/build/aac2mp4+0x41c349)

0x62d000008400 is located 0 bytes to the right of 32768-byte region
[0x62d000000400,0x62d000008400)
allocated by thread T0 here:
    #0 0x4f4638 in operator new[](unsigned long) /llvm-project/compiler-
rt/lib/asan/asan_new_delete.cpp:102
    #1 0x4fa30d in AP4_BitStream::AP4_BitStream() /Bento4/Source/C++/Codecs/Ap4BitStream.cpp:45:16
    #2 0x7fec98881c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

SUMMARY: AddressSanitizer: heap-buffer-overflow /llvm-project/compiler-
rt/lib/asan/asan_interceptors_memintrinsics.cpp:22 in __asan_memcpy
Shadow bytes around the buggy address:
  0x0c5a7fff9030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5a7fff9040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5a7fff9050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c5a7fff9060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0c5a7fff9070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c5a7fff9080:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5a7fff9090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5a7fff90a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5a7fff90b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5a7fff90c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5a7fff90d0: 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
==813117==ABORTING
```

Bug2

```
root@d5f4647d38bd:/aac2mp4/aac2mp4# ./mp4split crash2
no movie found in file

=================================================================
==888268==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 48 byte(s) in 1 object(s) allocated from:
    #0 0x4f45d8 in operator new(unsigned long) /llvm-project/compiler-
rt/lib/asan/asan_new_delete.cpp:99
    #1 0x5de94f in AP4_StdcFileByteStream::Create(AP4_FileByteStream*, char const*,
AP4_FileByteStream::Mode, AP4_ByteStream*&)
/Bento4/Source/C++/System/StdC/Ap4StdCFileByteStream.cpp:279:14

Indirect leak of 256 byte(s) in 1 object(s) allocated from:
    #0 0x4f45d8 in operator new(unsigned long) /llvm-project/compiler-
rt/lib/asan/asan_new_delete.cpp:99
    #1 0x536495 in AP4_Array<unsigned int>::EnsureCapacity(unsigned int)
/Bento4/Source/C++/Core/Ap4Array.h:172:25
    #2 0x536495 in AP4_Array<unsigned int>::Append(unsigned int const&)
/Bento4/Source/C++/Core/Ap4Array.h:252:29
```

```
    #3 0x536495 in AP4_FtypAtom::AP4_FtypAtom(unsigned int, AP4_ByteStream&)
/Bento4/Source/C++/Core/Ap4FtypAtom.cpp:57:28
    #4 0x50966b in AP4_FtypAtom::Create(unsigned int, AP4_ByteStream&)
/Bento4/Source/C++/Core/Ap4FtypAtom.h:66:20
    #5 0x50966b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) /Bento4/Source/C++/Core/Ap4AtomFactory.cpp:630:20
    #6 0x507ec4 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14
    #7 0x5076ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&)
/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:154:12
    #8 0x5350be in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool)
/Bento4/Source/C++/Core/Ap4File.cpp:104:12
    #9 0x5357ed in AP4_File::AP4_File(AP4_ByteStream&, bool)
/Bento4/Source/C++/Core/Ap4File.cpp:78:5
    #10 0x4f841f in main /Bento4/Source/C++/Apps/Mp4Split/Mp4Split.cpp:258:26
    #11 0x7f11ba50dc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 88 byte(s) in 1 object(s) allocated from:
    #0 0x4f45d8 in operator new(unsigned long) /llvm-project/compiler-
rt/lib/asan/asan_new_delete.cpp:99
    #1 0x507f57 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /Bento4/Source/C++/Core/Ap4AtomFactory.cpp:242:16
    #2 0x5076ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&)
/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:154:12
    #3 0x5350be in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool)
/Bento4/Source/C++/Core/Ap4File.cpp:104:12
    #4 0x5357ed in AP4_File::AP4_File(AP4_ByteStream&, bool)
/Bento4/Source/C++/Core/Ap4File.cpp:78:5
    #5 0x4f841f in main /Bento4/Source/C++/Apps/Mp4Split/Mp4Split.cpp:258:26
    #6 0x7f11ba50dc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 72 byte(s) in 1 object(s) allocated from:
    #0 0x4f45d8 in operator new(unsigned long) /llvm-project/compiler-
rt/lib/asan/asan_new_delete.cpp:99
    #1 0x4f83f7 in main /Bento4/Source/C++/Apps/Mp4Split/Mp4Split.cpp:258:22
    #2 0x7f11ba50dc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 72 byte(s) in 1 object(s) allocated from:
    #0 0x4f45d8 in operator new(unsigned long) /llvm-project/compiler-
rt/lib/asan/asan_new_delete.cpp:99
    #1 0x509659 in AP4_FtypAtom::Create(unsigned int, AP4_ByteStream&)
/Bento4/Source/C++/Core/Ap4FtypAtom.h:66:16
    #2 0x509659 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) /Bento4/Source/C++/Core/Ap4AtomFactory.cpp:630:20
    #3 0x507ec4 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14
    #4 0x5076ee in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&)
/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:154:12
    #5 0x5350be in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool)
/Bento4/Source/C++/Core/Ap4File.cpp:104:12
    #6 0x5357ed in AP4_File::AP4_File(AP4_ByteStream&, bool)
/Bento4/Source/C++/Core/Ap4File.cpp:78:5
    #7 0x4f841f in main /Bento4/Source/C++/Apps/Mp4Split/Mp4Split.cpp:258:26
    #8 0x7f11ba50dc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 48 byte(s) in 2 object(s) allocated from:
```

```
    #0 0x4f45d8 in operator new(unsigned long) /llvm-project/compiler-
rt/lib/asan/asan_new_delete.cpp:99
    #1 0x4fd2d3 in AP4_List<AP4_Atom>::Add(AP4_Atom*) /Bento4/Source/C++/Core/Ap4List.h:160:16
    #2 0x4fd2d3 in AP4_AtomParent::AddChild(AP4_Atom*, int)
/Bento4/Source/C++/Core/Ap4Atom.cpp:532:29

SUMMARY: AddressSanitizer: 584 byte(s) leaked in 7 allocation(s).
```

Environment

Ubuntu 18.04(docker)
clang 12.0.1
clang++ 12.0.1
Bento4 master branch(5b7cc25)

How to reproduce

```
export CC=clang
export CXX=clang++
export CFLAGS="-fsanitize=address -g"
export CXXFLAGS="-fsanitize=address -g"
mkdir build
cd build
cmake -DCMAKE_BUILD_TYPE=Release ..
make
```

POC

crash.zip

Credit

Yuhang Huang (NCNIPC of China)
Han Zheng (NCNIPC of China, Hexhive)
Yin li,Jiayu Zhao(NCNIPC of China)

Notice

I find the two bugs not only exist in latest branch but also exist in latest release version Bento4-1.6.0-639. The bug1 is similar to the issuse#363(CVE-2019-8378),which means this bug hasn't been fixed now.

Thanks for your time!

yuhanghuang changed the title ~~there are some bugsin Bento4~~ **there are some bugs in Bento4** on Sep 25

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant