New issue

Jump to bottom

Some vulnerabilities about mp4xx can cause serious errors #772

Open DylanSec opened this issue on Sep 23 · 0 comments

DylanSec commented on Sep 23 • edited

Summary

Hi there,
These are some faults that maybe lead to serious consequences in mp4xx, the version of Bento4 is the latest (the newest master branch) and the operation system is Ubuntu 18.04.6 LTS (docker), these binary-crashes with the following.

Bug1

Detected memory leaks in mp4spilt:

```
root@32345fj4sds:/fuzz-mp4split/mp4split# ./mp4split --video ../out/crashes/poc_split_1
--video option specified, but no video track found

=================================================================
==1889275==ERROR: LeakSanitizer: detected memory leaks

Indirect leak of 592 byte(s) in 2 object(s) allocated from:
    #0 0x8c7670 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x7f88d8e08297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
    #2 0x462e2f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/fuzz-mp4split/mp4split/mp4split+0x462e2f)
    #3 0x48ef27 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/fuzz-mp4split/mp4split/mp4split+0x48ef27)
    #4 0x490c11 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/fuzz-mp4split/mp4split/mp4split+0x490c11)

Indirect leak of 256 byte(s) in 1 object(s) allocated from:
    #0 0x8c7670 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
```

```
    #1 0x7f88d8e08297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
    #2 0x45904a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/fuzz-mp4split/mp4split/mp4split+0x45904a)
    #3 0x462a0f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/fuzz-mp4split/mp4split/mp4split+0x462a0f)
    #4 0x46094f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) (/fuzz-
mp4split/mp4split/mp4split+0x46094f)
    #5 0x4c4b30 in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) (/fuzz-
mp4split/mp4split/mp4split+0x4c4b30)
    #6 0x4c6558 in AP4_File::AP4_File(AP4_ByteStream&, bool) (/fuzz-
mp4split/mp4split/mp4split+0x4c6558)
    #7 0x40abba in main (/fuzz-mp4split/mp4split/mp4split+0x40abba)
    #8 0x7f88d878dc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 224 byte(s) in 7 object(s) allocated from:
    #0 0x8c7670 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x7f88d8e08297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
    #2 0x4c6558 in AP4_File::AP4_File(AP4_ByteStream&, bool) (/fuzz-
mp4split/mp4split/mp4split+0x4c6558)
    #3 0x40abba in main (/fuzz-mp4split/mp4split/mp4split+0x40abba)
    #4 0x7f88d878dc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 192 byte(s) in 2 object(s) allocated from:
    #0 0x8c7670 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x7f88d8e08297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
    #2 0x462a0f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/fuzz-mp4split/mp4split/mp4split+0x462a0f)
    #3 0x46094f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) (/fuzz-
mp4split/mp4split/mp4split+0x46094f)
    #4 0x4c4b30 in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) (/fuzz-
mp4split/mp4split/mp4split+0x4c4b30)
    #5 0x4c6558 in AP4_File::AP4_File(AP4_ByteStream&, bool) (/fuzz-
mp4split/mp4split/mp4split+0x4c6558)
    #6 0x40abba in main (/fuzz-mp4split/mp4split/mp4split+0x40abba)
    #7 0x7f88d878dc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 176 byte(s) in 2 object(s) allocated from:
    #0 0x8c7670 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x7f88d8e08297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
    #2 0x46094f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) (/fuzz-
mp4split/mp4split/mp4split+0x46094f)
    #3 0x4c4b30 in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) (/fuzz-
mp4split/mp4split/mp4split+0x4c4b30)
    #4 0x4c6558 in AP4_File::AP4_File(AP4_ByteStream&, bool) (/fuzz-
mp4split/mp4split/mp4split+0x4c6558)
    #5 0x40abba in main (/fuzz-mp4split/mp4split/mp4split+0x40abba)
    #6 0x7f88d878dc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
                                                                                    ……
……

Indirect leak of 24 byte(s) in 1 object(s) allocated from:
    #0 0x8c7670 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
```

```
    #1 0x7f88d8e08297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
    #2 0x4bdd4d in AP4_ElstAtom::Create(unsigned int, AP4_ByteStream&) (/fuzz-
mp4split/mp4split/mp4split+0x4bdd4d)
    #3 0x45831c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/fuzz-mp4split/mp4split/mp4split+0x45831c)
    #4 0x462a0f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/fuzz-mp4split/mp4split/mp4split+0x462a0f)
    #5 0x48ef27 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/fuzz-mp4split/mp4split/mp4split+0x48ef27)
    #6 0x48e726 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/fuzz-mp4split/mp4split/mp4split+0x48e726)
    #7 0x45dc8c in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/fuzz-mp4split/mp4split/mp4split+0x45dc8c)
    #8 0x462a0f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/fuzz-mp4split/mp4split/mp4split+0x462a0f)
    #9 0x48ef27 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/fuzz-mp4split/mp4split/mp4split+0x48ef27)
    #10 0x490c11 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/fuzz-mp4split/mp4split/mp4split+0x490c11)

Indirect leak of 1 byte(s) in 1 object(s) allocated from:
    #0 0x8c7670 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x7f88d8e08297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
    #2 0x771319 in AP4_DescriptorFactory::CreateDescriptorFromStream(AP4_ByteStream&,
AP4_Descriptor*&) (/fuzz-mp4split/mp4split/mp4split+0x771319)
    #3 0x539cf7 in AP4_InitialObjectDescriptor::AP4_InitialObjectDescriptor(AP4_ByteStream&,
unsigned char, unsigned int, unsigned int) (/fuzz-mp4split/mp4split/mp4split+0x539cf7)
    #4 0x7713f7 in AP4_DescriptorFactory::CreateDescriptorFromStream(AP4_ByteStream&,
AP4_Descriptor*&) (/fuzz-mp4split/mp4split/mp4split+0x7713f7)
    #5 0x4e9d46 in AP4_IodsAtom::Create(unsigned int, AP4_ByteStream&) (/fuzz-
mp4split/mp4split/mp4split+0x4e9d46)
    #6 0x4558fa in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) (/fuzz-mp4split/mp4split/mp4split+0x4558fa)
    #7 0x462a0f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) (/fuzz-mp4split/mp4split/mp4split+0x462a0f)
    #8 0x48ef27 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) (/fuzz-mp4split/mp4split/mp4split+0x48ef27)
    #9 0x490c11 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) (/fuzz-mp4split/mp4split/mp4split+0x490c11)

SUMMARY: AddressSanitizer: 2750 byte(s) leaked in 39 allocation(s).
```

Bug2

SEGV on unknown address 0x000000000028 in mp4decrypt:

```
root@23435332df4:/fuzz-mp4decrypt/mp4decrypt# ./mp4decrypt ../out/crashes/poc_decrypt_1 /dev/null
WARNING: atom serialized to fewer bytes than declared size
AddressSanitizer:DEADLYSIGNAL
```

```
=================================================================
==2367709==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000028 (pc 0x0000005da294 bp
0x7ffcee6b84c0 sp 0x7ffcee6b6b60 T0)
==2367709==The signal is caused by a READ memory access.
==2367709==Hint: address points to the zero page.
    #0 0x5da294 in AP4_Processor::ProcessFragments(AP4_MoovAtom*, AP4_List<AP4_AtomLocator>&,
AP4_ContainerAtom*, AP4_SidxAtom*, unsigned long long, AP4_ByteStream&, AP4_ByteStream&) (/fuzz-
mp4decrypt/mp4decrypt/mp4decrypt+0x5da294)
    #1 0x5f795d in AP4_Processor::Process(AP4_ByteStream&, AP4_ByteStream&, AP4_ByteStream*,
AP4_Processor::ProgressListener*, AP4_AtomFactory&) (/fuzz-
mp4decrypt/mp4decrypt/mp4decrypt+0x5f795d)
    #2 0x414e8b in main (/fuzz-mp4decrypt/mp4decrypt/mp4decrypt+0x414e8b)
    #3 0x7fdba0338c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #4 0x407b69 in _start (/fuzz-mp4decrypt/mp4decrypt/mp4decrypt+0x407b69)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/fuzz-mp4decrypt/mp4decrypt/mp4decrypt+0x5da294) in
AP4_Processor::ProcessFragments(AP4_MoovAtom*, AP4_List<AP4_AtomLocator>&, AP4_ContainerAtom*,
AP4_SidxAtom*, unsigned long long, AP4_ByteStream&, AP4_ByteStream&)
==2367709==ABORTING
```

Bug3

Detected memory leaks in mp4mux:

```
root@wha446aq:/# ./Bento4/cmakebuild/mp4mux --track h264:poc_mp4mux_1 /dev/null
ERROR: Feed() failed (-10)

=================================================================
==17429==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 148 byte(s) in 1 object(s) allocated from:
    #0 0x4f5ce8 in operator new(unsigned long) /llvm-project/compiler-
rt/lib/asan/asan_new_delete.cpp:99
    #1 0x52d6b2 in AP4_AvcFrameParser::Feed(unsigned char const*, unsigned int,
AP4_AvcFrameParser::AccessUnitInfo&, bool) (/Bento4/cmakebuild/mp4mux+0x52d6b2)

SUMMARY: AddressSanitizer: 148 byte(s) leaked in 1 allocation(s).
```

POC

Bug_1_POC.zip
Bug_2_POC.zip
Bug_3_POC.zip

Environment

Ubuntu 18.04.6 LTS (docker)
clang 12.0.1
clang++ 12.0.1
Bento4 master branch(`5b7cc25`) && Bento4 release version(1.6.0-639)

Credit

Xudong Cao (NCNIPC of China)
Han Zheng (NCNIPC of China, Hexhive)
Yuhang Huang (NCNIPC of China)
Jiayuan Zhang (NCNIPC of China)

Thank you for your time!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant