

New issue

[Jump to bottom](#)

Detected memory leaks in mp4encrypt #766

Open DylanSec opened this issue on Sep 19 · 0 comments

DylanSec commented on Sep 19 • edited ▾

Summary

Hi, developers of Bento4:

I tested the binary mp4encrypt, and a crash incurred, i.e., memory leaks error. The version of Bento4 is the latest (the newest master branch) and the operation system is Ubuntu 18.04.6 LTS (docker). The following is the details.

Details

```
root@c08635047aea:/fuzz-mp4encrypt/mp4encrypt# ./mp4encrypt --method MARLIN-IPMP-ACBC
../out/crashes/id\:000007\,sig\:06\,src\:000001\,op\:flip1\,pos\:14136\,934837 /dev/null
WARNING: track ID 1 will not be encrypted
WARNING: atom serialized to fewer bytes than declared size
```

```
=====
==3055140==ERROR: LeakSanitizer: detected memory leaks
```

Direct leak of 104 byte(s) in 1 object(s) allocated from:

```
#0 0x9a1c90 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
#1 0x7fda31f4c297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
#2 0x64923f in AP4_Processor::Process(AP4_ByteStream&, AP4_ByteStream&, AP4_ByteStream*,
AP4_Processor::ProgressListener*, AP4_AtomFactory&) (/fuzz-
mp4encrypt/mp4encrypt/mp4encrypt+0x64923f)
#3 0x42128c in main (/fuzz-mp4encrypt/mp4encrypt/mp4encrypt+0x42128c)
#4 0x7fda31110c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
```

Indirect leak of 3328 byte(s) in 2 object(s) allocated from:

```
#0 0x9a1c90 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
#1 0x7fda31f4c297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
#2 0x5b2921 in AP4_MarlinIpmpeEncryptingProcessor::Initialize(AP4_AtomParent&, AP4_ByteStream&,
```

```
AP4_Processor::ProgressListener*) (/fuzz-mp4encrypt/mp4encrypt/mp4encrypt+0x5b2921)
#3 0x64923f in AP4_Processor::Process(AP4_ByteStream&, AP4_ByteStream&, AP4_ByteStream*,
AP4_Processor::ProgressListener*, AP4_AtomFactory&) (/fuzz-
mp4encrypt/mp4encrypt/mp4encrypt+0x64923f)
#4 0x42128c in main (/fuzz-mp4encrypt/mp4encrypt/mp4encrypt+0x42128c)
#5 0x7fda31110c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 1024 byte(s) in 1 object(s) allocated from:
#0 0x9a1c90 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
#1 0x7fda31f4c297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
#2 0x8b62f9 in AP4_Expandable::Write(AP4_ByteStream&) (/fuzz-
mp4encrypt/mp4encrypt/mp4encrypt+0x8b62f9)
#3 0x5b2540 in AP4_MarlinIcmpEncryptingProcessor::Initialize(AP4_AtomParent&, AP4_ByteStream&,
AP4_Processor::ProgressListener*) (/fuzz-mp4encrypt/mp4encrypt/mp4encrypt+0x5b2540)
#4 0x64923f in AP4_Processor::Process(AP4_ByteStream&, AP4_ByteStream&, AP4_ByteStream*,
AP4_Processor::ProgressListener*, AP4_AtomFactory&) (/fuzz-
mp4encrypt/mp4encrypt/mp4encrypt+0x64923f)
#5 0x42128c in main (/fuzz-mp4encrypt/mp4encrypt/mp4encrypt+0x42128c)
#6 0x7fda31110c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 224 byte(s) in 5 object(s) allocated from:
#0 0x9a1c90 in malloc /llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
#1 0x7fda31f4c297 in operator new(unsigned long) (/usr/lib/x86_64-linux-
gnu/libstdc++.so.6+0x93297)
#2 0x64923f in AP4_Processor::Process(AP4_ByteStream&, AP4_ByteStream&, AP4_ByteStream*,
AP4_Processor::ProgressListener*, AP4_AtomFactory&) (/fuzz-
mp4encrypt/mp4encrypt/mp4encrypt+0x64923f)
#3 0x42128c in main (/fuzz-mp4encrypt/mp4encrypt/mp4encrypt+0x42128c)
#4 0x7fda31110c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

SUMMARY: AddressSanitizer: 4680 byte(s) leaked in 9 allocation(s).
```

POC

[mp4encrypt_poc1.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](#))

Thank you for your time!

 **DylanSec** closed this as completed on Oct 2

 **DylanSec** reopened this on Oct 4

  **DylanSec** mentioned this issue on Oct 6

Some Memory leaks exist in mp4xx #792

 **Open**

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

