

[New issue](#)
[Jump to bottom](#)

# Memory leaks with ASAN in mp42aac #788

Open 17ssDP opened this issue on Oct 4 · 0 comments

17ssDP commented on Oct 4

Hi, developers of Bento4:

In the test of the binary mp42aac instrumented with ASAN. There are some inputs causing memory leaks. Here is the ASAN mode output. The output is different from [#763](#).

```
=====
==6659==ERROR: LeakSanitizer: detected memory leaks
```

Direct leak of 64 byte(s) in 1 object(s) allocated from:

#0 0x7f8d891f0592 in operator new(unsigned long) (/usr/lib/x86\_64-linux-gnu/libasan.so.2+0x99592)

[#1](#) 0x418dff in AP4\_File::ParseStream(AP4\_ByteStream&, AP4\_AtomFactory&, bool)

/root/Bento4/Source/C++/Core/Ap4File.cpp:108

[#2](#) 0x418dff in AP4\_File::AP4\_File(AP4\_ByteStream&, bool) /root/Bento4/Source/C++/Core/Ap4File.cpp:78

SUMMARY: AddressSanitizer: 64 byte(s) leaked in 1 allocation(s).

## Crash Input

[https://github.com/17ssDP/fuzzer\\_crashes/blob/main/Bento4/mp42aac-ml-01](https://github.com/17ssDP/fuzzer_crashes/blob/main/Bento4/mp42aac-ml-01)

## Verification steps:

```
git clone https://github.com/axiomatic-systems/Bento4
```

```
cd Bento4/
```

```
mkdir check_build && cd check_build
```

```
cmake ../ -DCMAKE_C_COMPILER=clang -DCMAKE_CXX_COMPILER=clang++ -DCMAKE_C_FLAGS="-
```

```
fsanitize=address" -DCMAKE_CXX_FLAGS="-fsanitize=address" -DCMAKE_BUILD_TYPE=Release
```

```
make -j
```

```
./mp42aac mp42aac-ml-01 /dev/null
```

## Environment

Ubuntu 16.04

Clang 10.0.1

gcc 5.5

#### Assignees

No one assigned

---

#### Labels

None yet

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

1 participant

