

New issue

[Jump to bottom](#)

# Some heap buffer overflow bugs exist in avcinfo #794

🔓 Open burymyname opened this issue on Oct 10 · 0 comments

burymyname commented on Oct 10

Hello, developers of Bento4!

I also found some **heap buffer overflow** bugs in avcinfo by using our fuzzing tools with ASAN.

Here is details:

## Bug1

```
=====
==48171==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000038 at pc
0x7f1ff86b4733 bp 0x7fff66ab01b0 sp 0x7fff66aaf958
READ of size 8 at 0x602000000038 thread T0
    #0 0x7f1ff86b4732 (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79732)
    #1 0x5638f29e7432 in AP4_BitStream::WriteBytes(unsigned char const*, unsigned int)
Bento4/Source/C++/Codecs/Ap4BitStream.cpp:133
    #2 0x5638f29c0c69 in PrintSliceInfo Bento4/Source/C++/Apps/AvcInfo/AvcInfo.cpp:84
    #3 0x5638f29c0c69 in main Bento4/Source/C++/Apps/AvcInfo/AvcInfo.cpp:172
    #4 0x7f1ff7ccac86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #5 0x5638f29c1679 in _start (Bento4/avcinfo+0x5679)

0x602000000038 is located 0 bytes to the right of 8-byte region [0x602000000030,0x602000000038)
allocated by thread T0 here:
    #0 0x7f1ff871b608 in operator new[](unsigned long) (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xe0608)
    #1 0x5638f29ed326 in AP4_DataBuffer::ReallocateBuffer(unsigned int)
Bento4/Source/C++/Core/Ap4DataBuffer.cpp:210
    #2 0x5638f29ed326 in AP4_DataBuffer::SetDataSize(unsigned int)
Bento4/Source/C++/Core/Ap4DataBuffer.cpp:151

SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79732)
Shadow bytes around the buggy address:
  0x0c047fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c047fff8000: fa fa fd fa fa fa 00[fa]fa fa fa fa fa fa fa fa
```

```

0x0c047fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8050: 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
==48171==ABORTING

```

## Poc

[avcinfo\\_poc1.zip](#)

## Bug2

---

```

=====
==48988==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000011 at pc
0x561df275ee6e bp 0x7ffca5855570 sp 0x7ffca5855560
READ of size 1 at 0x602000000011 thread T0
#0 0x561df275ee6d in main Bento4/Source/C++/Apps/AvcInfo/AvcInfo.cpp:166
#1 0x7f9a9fbd8c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
#2 0x561df275f679 in _start (Bento4/avcinfo+0x5679)

0x602000000011 is located 0 bytes to the right of 1-byte region [0x602000000010,0x602000000011)
allocated by thread T0 here:
#0 0x7f9aa0629608 in operator new[](unsigned long) (/usr/lib/x86_64-linux-
gnu/libasan.so.4+0xe0608)
#1 0x561df278b326 in AP4_DataBuffer::ReallocateBuffer(unsigned int)
Bento4/Source/C++/Core/AP4DataBuffer.cpp:210
#2 0x561df278b326 in AP4_DataBuffer::SetDataSize(unsigned int)
Bento4/Source/C++/Core/AP4DataBuffer.cpp:151

SUMMARY: AddressSanitizer: heap-buffer-overflow Bento4/Source/C++/Apps/AvcInfo/AvcInfo.cpp:166 in
main
Shadow bytes around the buggy address:

```

```
0x0c047fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c047fff8000: fa fa[01]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8050: fa 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
```

```
==48988==ABORTING
```

## PoC

[avcinfo\\_poc2.zip](#)

## 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
./avcinfo poc
```

## Environment

---

- Ubuntu 18.04
- clang 10.01
- Bento4 master branch [4df7274e](#) commit and version 1.6.0-639

Thanks for your time!

#### Assignees

No one assigned

---

#### Labels

None yet

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

1 participant

