New issue

Heap-buffer-overflow in AP4_Dac4Atom DSI v1 parsing via large n_presentations (AP4_BitReader::SkipBits) #1059

Open

BreakingBad6 opened 2 weeks ago

A heap-buffer-overflow vulnerability exists in the `AP4_Dac4Atom` constructor when parsing AC-4 DSI version 1 data. A crafted MP4 file with a `dac4` atom containing a large `n_presentations` value (up to 511) causes the parser to read far beyond the allocated heap buffer via `AP4_BitReader::SkipBits()`.

Affected Component

- File: `Source/C++/Core/Ap4Dac4Atom.cpp`
- Function: `AP4_Dac4Atom::AP4_Dac4Atom(AP4_UI32 size, const AP4_UI08* payload)` (line 147)
- Triggered at: `AP4_BitReader::SkipBits()` in `Ap4Utils.cpp:559`, called from `Ap4Dac4Atom.cpp:396`

Root Cause

In `Ap4Dac4Atom.cpp`, the DSI v1 parsing path reads `n_presentations` from 9 bits (line 175), allowing a maximum value of 511. At line 196, an array of `PresentationV1[n_presentations]` is allocated and each element is parsed in a loop (line 198). Each presentation parsing iteration calls `ReadBits()` and `SkipBits()` multiple times. When the actual payload is much smaller than what 511 presentations require, the `AP4_BitReader` reads and skips well past the end of the heap-allocated buffer without any bounds checking.

Steps to Reproduce

1. Build Bento4 with AddressSanitizer (`-fsanitize=address`)
2. Save the attached PoC file as `poc3.mp4`
3. Run: `./mp4dump poc3.mp4`

ASAN Output

```
==3552==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x5030000002f4
at pc 0x58993d791c01 bp 0x7fffc0067da0 sp 0x7fffc0067d90
READ of size 1 at 0x5030000002f4 thread T0
    #0 AP4_BitReader::ReadCache() const  Ap4Utils.cpp:447
    #1 AP4_BitReader::SkipBits()         Ap4Utils.cpp:559
    #2 AP4_Dac4Atom::AP4_Dac4Atom()      Ap4Dac4Atom.cpp:396
    #3 AP4_Dac4Atom::Create()            Ap4Dac4Atom.cpp:58

0x5030000002f4 is located 0 bytes to the right of 20-byte region
[0x5030000002e0,0x5030000002f4)
```

(Full ASAN trace and PoC file attached below)

Impact

An attacker can craft a malicious MP4 file that, when parsed by any application using the Bento4 library (e.g., mp4dump, mp4info), triggers a heap out-of-bounds read. This may lead to information disclosure or denial of service (crash).

Suggested Fix

Add remaining-bits validation during the presentation parsing loop:

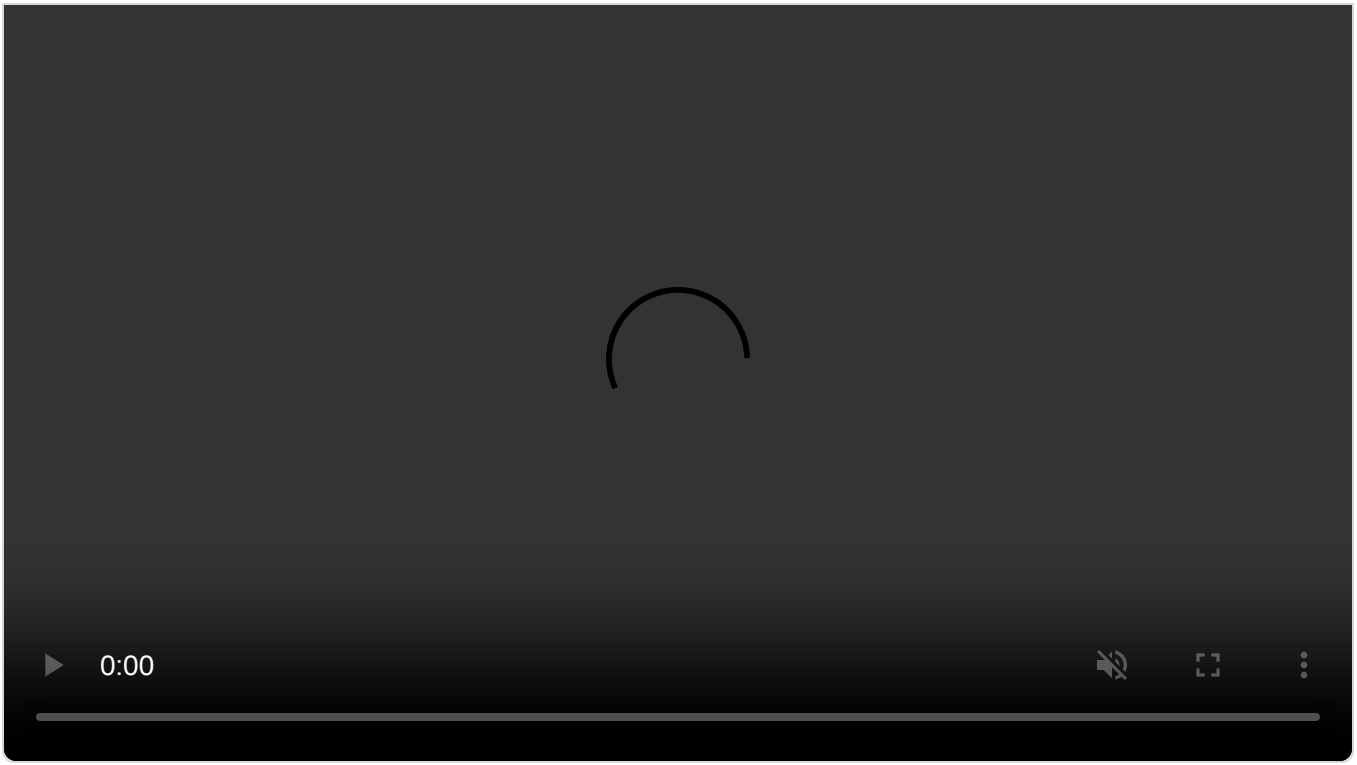
```
// Ap4Dac4Atom.cpp, before line 198
// Limit n_presentations to what the payload can actually hold
for (unsigned int i = 0; i < m_Dsi.d.v1.n_presentations; i++) {
    if (bits.GetBitsRead() >= payload_size * 8) break;  // prevent OOB
    // ... existing parsing code ...
}
```

Additionally, `AP4_BitReader` should return an error or stop when the read position exceeds the buffer size.

Environment

- Bento4 version: latest (commit HEAD)
- OS: Ubuntu (WSL2)
- Compiler: g++ with `-fsanitize=address`

poc3_dac4_heap_oob.mp4


0:00

```
breakingbad@LAPTOP-H9E173A0:/mnt/c/Users/18320/Desktop/新农计划/example/Bento4/cmakebuild$ cp /mnt/c/Users/18320/Desktop
/新农计划/poc/*.mp4 .
breakingbad@LAPTOP-H9E173A0:/mnt/c/Users/18320/Desktop/新农计划/example/Bento4/cmakebuild$ ./mp4dump poc3_dac4_heap_oob.
mp4
[ftyp] size=8+12
  major_brand = isom
  minor_version = 200
  compatible_brand = isom
=================================================================
==3552==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x5030000002f4 at pc 0x58993d791c01 bp 0x7fffc0067da0 s
p 0x7fffc0067d90
READ of size 1 at 0x5030000002f4 thread T0
    #0 0x58993d791c00 in AP4_BitReader::ReadCache() const /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/
Core/Ap4Utils.cpp:447
    #1 0x58993d792496 in AP4_BitReader::SkipBits(unsigned int) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source
/C++/Core/Ap4Utils.cpp:559
    #2 0x58993d6f9679 in AP4_Dac4Atom::AP4_Dac4Atom(unsigned int, unsigned char const*) /mnt/c/Users/18320/Desktop/新农
计划/example/Bento4/Source/C++/Core/Ap4Dac4Atom.cpp:396
    #3 0x58993d6f5598 in AP4_Dac4Atom::Create(unsigned int, AP4_ByteStream&) /mnt/c/Users/18320/Desktop/新农计划/example
/Bento4/Source/C++/Core/Ap4Dac4Atom.cpp:58
    #4 0x58993d6e128a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned lon
g long, AP4_Atom*&) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:776
    #5 0x58993d6dd61f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/c/
Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #6 0x58993d6f07b2 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /mnt/c/U
sers/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:196
    #7 0x58993d75ef53 in AP4_SampleEntry::Read(AP4_ByteStream&, AP4_AtomFactory&) /mnt/c/Users/18320/Desktop/新农计划/ex
ample/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:115
    #8 0x58993d760af2 in AP4_AudioSampleEntry::AP4_AudioSampleEntry(unsigned int, unsigned int, AP4_ByteStream&, AP4_Ato
mFactory&) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:420
    #9 0x58993d762fa0 in AP4_Ac4SampleEntry::AP4_Ac4SampleEntry(unsigned int, unsigned int, AP4_ByteStream&, AP4_AtomFac
tory&) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:801
    #10 0x58993d6de436 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned lo
ng long, AP4_Atom*&) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:342
    #11 0x58993d6dd61f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/c
/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #12 0x58993d774bc2 in AP4_StsdAtom::AP4_StsdAtom(unsigned int, unsigned char, unsigned int, AP4_ByteStream&, AP4_Ato
mFactory&) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:104
    #42 0x58993d6dd61f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mn
/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #43 0x58993d6dcbed in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) /mnt/c/Users/18320/Deskt
新农计划/example/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:154
    #44 0x58993d6cf3ed in main /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Apps/Mp4Dump/Mp4Dump.cpp
2
    #45 0x7b77d3829d8f in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
    #46 0x7b77d3829e3f in __libc_start_main_impl ../csu/libc-start.c:392
    #47 0x58993d6cd904 in _start (/mnt/c/Users/18320/Desktop/新农计划/example/Bento4/cmakebuild/mp4dump+0x319904)

0x5030000002f4 is located 0 bytes to the right of 20-byte region [0x5030000002e0,0x5030000002f4)
allocated by thread T0 here:
    #0 0x7b77d40b6357 in operator new[](unsigned long) ../../../../src/libsanitizer/asan/asan_new_delete.cpp:102
    #1 0x58993d70564c in AP4_DataBuffer::ReallocateBuffer(unsigned int) /mnt/c/Users/18320/Desktop/新农计划/example/B
o4/Source/C++/Core/Ap4DataBuffer.cpp:210
    #2 0x58993d7052a0 in AP4_DataBuffer::SetBufferSize(unsigned int) /mnt/c/Users/18320/Desktop/新农计划/example/Bent
Source/C++/Core/Ap4DataBuffer.cpp:136
    #3 0x58993d791928 in AP4_BitReader::AP4_BitReader(unsigned char const*, unsigned int) /mnt/c/Users/18320/Desktop/
农计划/example/Bento4/Source/C++/Core/Ap4Utils.cpp:404
    #4 0x58993d6f6986 in AP4_Dac4Atom::AP4_Dac4Atom(unsigned int, unsigned char const*) /mnt/c/Users/18320/Desktop/新
计划/example/Bento4/Source/C++/Core/Ap4Dac4Atom.cpp:161
    #5 0x58993d6f5598 in AP4_Dac4Atom::Create(unsigned int, AP4_ByteStream&) /mnt/c/Users/18320/Desktop/新农计划/exam
/Bento4/Source/C++/Core/Ap4Dac4Atom.cpp:58
    #6 0x58993d6e128a in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned
g long, AP4_Atom*&) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:776
    #7 0x58993d6dd61f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt
Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234
    #8 0x58993d6f07b2 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /mnt/
sers/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:196
    #9 0x58993d75ef53 in AP4_SampleEntry::Read(AP4_ByteStream&, AP4_AtomFactory&) /mnt/c/Users/18320/Desktop/新农计划
ample/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:115
    #10 0x58993d760af2 in AP4_AudioSampleEntry::AP4_AudioSampleEntry(unsigned int, unsigned int, AP4_ByteStream&, AP4
omFactory&) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:420
    #11 0x58993d762fa0 in AP4_Ac4SampleEntry::AP4_Ac4SampleEntry(unsigned int, unsigned int, AP4_ByteStream&, AP4_Ato
ctory&) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4SampleEntry.cpp:801
    #12 0x58993d6de436 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned
ng long, AP4_Atom*&) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:342
    #13 0x58993d6dd61f in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mn
```

```
    #29 0x58993d6f0131 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&,
AP4_AtomFactory&) /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:140

SUMMARY: AddressSanitizer: heap-buffer-overflow /mnt/c/Users/18320/Desktop/新农计划/example/Bento4/Source/C++/Core/Ap4Ut
ils.cpp:447 in AP4_BitReader::ReadCache() const
Shadow bytes around the buggy address:
  0x0a067fff8000: fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00
  0x0a067fff8010: 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
  0x0a067fff8020: 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa
  0x0a067fff8030: fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00
  0x0a067fff8040: 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
=>0x0a067fff8050: 00 00 04 fa fa fa 00 00 04 fa fa fa 00 00[04]fa
  0x0a067fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0a067fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0a067fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0a067fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0a067fff80a0: 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
==3552==ABORTING
breakingbad@LAPTOP-H9E173A0:/mnt/c/Users/18320/Desktop/新农计划/example/Bento4/cmakebuild$ ./mp42ts --index poc2_mfra_se
ek.mp4 /dev/null
ERROR: unexpected argument
breakingbad@LAPTOP-H9E173A0:/mnt/c/Users/18320/Desktop/新农计划/example/Bento4/cmakebuild$ ./mp42ts --index poc2_mfra_se
ek.mp4 /dev/null
ERROR: unexpected argument
breakingbad@LAPTOP-H9E173A0:/mnt/c/Users/18320/Desktop/新农计划/example/Bento4/cmakebuild$ ./mp4info poc2_mfra_seek.mp4
File:
```


Metadata

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants