

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

## Null pointer dereference caused by unhandled exhaustive memory usage #416

[Open](#) Shadowblad3 opened this issue on Aug 9, 2019 · 0 comments

Assignees



Labels

fuzzing

Shadowblad3 commented on Aug 9, 2019

There is a null pointer dereference caused by unhandled exhaustive memory usage in Ap48bdAtom.cpp.

Distributor ID: Ubuntu  
Description: Ubuntu 16.04.6 LTS  
Release: 16.04  
Codename: xenial  
gcc: 5.4.0

To reproduce the bug,  
compile the project with flag  
DCMAKE\_C\_FLAGS=-g -m32 -fsanitize=address,undefined

then run:  
./mp42aac input /dev/null

The reason is that the malloc size does not check and easily lead to memory allocation failure.

```
71 AP4_8bdAtom::AP4_8bdAtom(AP4_Size size,  
72 AP4_ByteStream& stream) :  
73 AP4_Atom(AP4_ATOM_TYPE_8BDL, (AP4_UI32)(size)),  
74 m_Encoding(AP4_8BDL_XML_DATA_ENCODING),  
75 m_EncodingVersion(0),  
76 m_BundleData(size-AP4_ATOM_HEADER_SIZE-8) initialize an null pointer  
77 {  
78 stream.ReadUI32(m_Encoding);  
79 stream.ReadUI32(m_EncodingVersion);  
80 m_BundleData.SetDataSize(m_BundleData.GetBufferSize());  
81 stream.Read(m_BundleData.UseData(), m_BundleData.GetDataSize());  
82 }  
83 null pointer dereference
```



```
49 AP4_DataBuffer::AP4_DataBuffer(AP4_Size buffer_size) :  
50 m_BufferIsLocal(true),  
51 m_Buffer(NULL),  
52 m_BufferSize(buffer_size),  
53 m_DataSize(0) return without checking  
54 {  
55 m_Buffer = new AP4_Byte[buffer_size];  
56 }
```

Here is the trace reported by ASAN:

```
==131030==WARNING: AddressSanitizer failed to allocate 0xffe1fff bytes  
==131030==AddressSanitizer's allocator is terminating the process instead of returning 0  
==131030==If you don't like this behavior set allocator_may_return_null=1  
==131030==AddressSanitizer CHECK failed: ././././src/libsanitizer/sanitizer_common/sanitizer_allocator.cc:147 "(0) != (0)" (0x0, 0x0)  
#0 0xf71fe797 (/usr/lib32/libasan.so.2+0x9f797)  
#1 0xf7203a69 in __sanitizer::CheckFailed(char const*, int, char const*, unsigned long long, unsigned long long) (/usr/lib32/libasan.so.2+0xa4a69)  
#2 0xf717507b (/usr/lib32/libasan.so.2+0x1607b)  
#3 0xf7201e80 (/usr/lib32/libasan.so.2+0xa2e80)  
#4 0xf717a229 (/usr/lib32/libasan.so.2+0x1b229)  
#5 0xf71f6e16 in operator new[](unsigned int) (/usr/lib32/libasan.so.2+0x97e16)  
#6 0x877ebaf in AP4_DataBuffer::AP4_DataBuffer(unsigned int) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4DataBuffer.cpp:55  
#7 0x8ba5673 in AP4_8bdAtom::AP4_8bdAtom(unsigned int, AP4_ByteStream&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap48bdAtom.cpp:76  
#8 0x8ba5673 in AP4_8bdAtom::Create(unsigned int, AP4_ByteStream&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap48bdAtom.cpp:64  
#9 0x82e10dc in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:534  
#10 0x8301ca3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225  
#11 0x82b6bae in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned long long) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:194  
#12 0x82b6bae in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4ContainerAtom.cpp:139  
#13 0x841a898 in AP4_MoovAtom::AP4_MoovAtom(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4MoovAtom.cpp:80  
#14 0x82e2631 in AP4_MoovAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4MoovAtom.h:56  
#15 0x82e2631 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned int, unsigned long long, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:363  
#16 0x82fa1f7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:225  
#17 0x82fa1f7 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4AtomFactory.cpp:151  
#18 0x809a044 in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4File.cpp:104  
#19 0x809a044 in AP4_File::AP4_File(AP4_ByteStream&, bool) /mnt/data/playground/mp42-a/Source/C++/Core/Ap4File.cpp:78  
#20 0x8082ce7 in main /mnt/data/playground/mp42-a/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:250  
#21 0xf697f636 in __libc_start_main (/lib32-linux-gnu/libc.so.6+0x18636)  
#22 0x808df1b (/mnt/data/playground/mp42-patch/Build/mp42aac+0x808df1b)
```

The poc input:  
[poc\\_input6.zip](#)

  **barbibulle** self-assigned this on Aug 25, 2019

  **barbibulle** added the **fuzzing** label on Aug 25, 2019

Assignees

 **barbibulle**

---

Labels

**fuzzing**

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

