

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

Heap overflow in mp4info, ReadPartial, Ap4StdCFileByteStream.cpp:341 #812

Open 5shadowblad3 opened this issue 15 days ago · 0 comments

5shadowblad3 commented 15 days ago • edited ▼

Hi, there.

There is an heap overflow in ReadPartial, Ap4StdCFileByteStream.cpp:341, in the newest master branch [5e7bb34](#), which seems to be incomplete fix of issue [#510](#).

Here is the reproducing command:

```
mp42info poc
```

POC:

[mp4info_overflow_ReadPartial341.zip](#)

(unzip first)

The reason of this overflow can causes arbitrary code execution by memory manipulation since user can control the content parsed by the program.

```
331 /*-----*/
332 |   AP4_StdCFileByteStream::ReadPartial
333 +-----*/
334 AP4_Result
335 AP4_StdCFileByteStream::ReadPartial(void*    buffer,
336                                     AP4_Size bytesToRead,
337                                     AP4_Size& bytesRead)
338 {
339     size_t nbRead;
340
341     nbRead = fread(buffer, 1, bytesToRead, m_File);
342
343     if (nbRead > 0) {
344         bytesRead = (AP4_Size)nbRead;
345         m_Position += nbRead;
346         return AP4_SUCCESS;
347     } else if (feof(m_File)) {
348         bytesRead = 0;
```

user can control the content parsed by the program

Here is the reproduce trace reported by ASAN:

```
==1448318==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000171 at pc
0x000000471d71 bp 0x7ffd4dd08e80 sp 0x7ffd4dd08630
WRITE of size 30 at 0x60200000171 thread T0
    #0 0x471d70 in __interceptor_fread.part.0 /dependence/llvm11/llvm-
11.0.0.src/projects/compiler-
rt/lib/asan/./sanitizer_common/sanitizer_common_interceptors.inc:1027:16
    #1 0x66f795 in AP4_StdcFileByteStream::ReadPartial(void*, unsigned int, unsigned int&)
/benchmark/Bento4/Source/C++/System/StdC/Ap4StdCFileByteStream.cpp:341:14
    #2 0x549ce9 in AP4_ByteStream::Read(void*, unsigned int)
/benchmark/Bento4/Source/C++/Core/Ap4ByteStream.cpp:54:29
    #3 0x6601bb in AP4_MetaDataStringAtom::AP4_MetaDataStringAtom(unsigned int, unsigned int,
AP4_ByteStream&) /benchmark/Bento4/Source/C++/MetaData/Ap4MetaData.cpp:1637:12
    #4 0x6601bb in AP4_MetaDataAtomTypeHandler::CreateAtom(unsigned int, unsigned int,
AP4_ByteStream&, unsigned int, AP4_Atom*&)
/benchmark/Bento4/Source/C++/MetaData/Ap4MetaData.cpp:428:24
    #5 0x53d50b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:844:21
    #6 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14
    #7 0x553677 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194:12
    #8 0x5529a3 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139:5
    #9 0x5529a3 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88:20
    #10 0x660634 in AP4_MetaDataAtomTypeHandler::CreateAtom(unsigned int, unsigned int,
AP4_ByteStream&, unsigned int, AP4_Atom*&)
/benchmark/Bento4/Source/C++/MetaData/Ap4MetaData.cpp:419:20
    #11 0x53d50b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:844:21
    #12 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14
    #13 0x553677 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194:12
    #14 0x5529a3 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139:5
    #15 0x5529a3 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88:20
    #16 0x53def3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816:20
    #17 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14
    #18 0x55389e in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194:12
    #19 0x552c6e in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
unsigned char, unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
/benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:154:5
    #20 0x552c6e in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:86:20
    #21 0x53dd0d in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:830:20
    #22 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14
```

```

#23 0x553677 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) /benchmark/Bento4/Source/C++/Core/AP4ContainerAtom.cpp:194:12
#24 0x5529a3 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/AP4ContainerAtom.cpp:139:5
#25 0x5529a3 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/AP4ContainerAtom.cpp:88:20
#26 0x53def3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/AP4AtomFactory.cpp:816:20
#27 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/AP4AtomFactory.cpp:234:14
#28 0x5746a6 in AP4_DrefAtom::AP4_DrefAtom(unsigned int, unsigned char, unsigned int,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/AP4DrefAtom.cpp:84:16
#29 0x573f60 in AP4_DrefAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)
/benchmark/Bento4/Source/C++/Core/AP4DrefAtom.cpp:50:16
#30 0x53ed78 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/AP4AtomFactory.cpp:580:20
#31 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/AP4AtomFactory.cpp:234:14
#32 0x553677 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) /benchmark/Bento4/Source/C++/Core/AP4ContainerAtom.cpp:194:12
#33 0x5529a3 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/AP4ContainerAtom.cpp:139:5
#34 0x5529a3 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/AP4ContainerAtom.cpp:88:20
#35 0x53def3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/AP4AtomFactory.cpp:816:20
#36 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/AP4AtomFactory.cpp:234:14
#37 0x53b237 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&)
/benchmark/Bento4/Source/C++/Core/AP4AtomFactory.cpp:154:12
#38 0x579c4b in AP4_File::ParseStream(AP4_ByteStream&, AP4_AtomFactory&, bool)
/benchmark/Bento4/Source/C++/Core/AP4File.cpp:104:12
#39 0x57a2ff in AP4_File::AP4_File(AP4_ByteStream&, bool)
/benchmark/Bento4/Source/C++/Core/AP4File.cpp:78:5
#40 0x4fb236 in main /benchmark/Bento4/Source/C++/Apps/Mp4Info/Mp4Info.cpp:1852:26
#41 0x7f2c774ff082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-
start.c:308:16
#42 0x41d89d in _start (/benchmark/Bento4/build-a/mp4info+0x41d89d)

```

0x60200000171 is located 0 bytes to the right of 1-byte region [0x60200000170,0x60200000171) allocated by thread T0 here:

```

#0 0x4f7fc7 in operator new[](unsigned long) /dependence/llvm11/llvm-
11.0.0.src/projects/compiler-rt/lib/asan/asan_new_delete.cpp:102:3
#1 0x60b04d in AP4_String::AP4_String(unsigned int)
/benchmark/Bento4/Source/C++/Core/AP4String.cpp:85:15
#2 0x53d50b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/AP4AtomFactory.cpp:844:21
#3 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&,
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/AP4AtomFactory.cpp:234:14
#4 0x553677 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned
long long) /benchmark/Bento4/Source/C++/Core/AP4ContainerAtom.cpp:194:12
#5 0x5529a3 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/AP4ContainerAtom.cpp:139:5
#6 0x5529a3 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/AP4ContainerAtom.cpp:88:20
#7 0x660634 in AP4_MetaDataAtomTypeHandler::CreateAtom(unsigned int, unsigned int,

```

```
AP4_ByteStream&, unsigned int, AP4_Atom*&)  
/benchmark/Bento4/Source/C++/MetaData/Ap4MetaData.cpp:419:20  
#8 0x53d50b in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned  
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:844:21  
#9 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&  
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14  
#10 0x553677 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned  
long long) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194:12  
#11 0x5529a3 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,  
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139:5  
#12 0x5529a3 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,  
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88:20  
#13 0x53def3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned  
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816:20  
#14 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&  
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14  
#15 0x55389e in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned  
long long) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194:12  
#16 0x552c6e in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,  
unsigned char, unsigned int, AP4_ByteStream&, AP4_AtomFactory&)  
/benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:154:5  
#17 0x552c6e in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,  
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:86:20  
#18 0x53dd0d in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned  
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:830:20  
#19 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&  
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14  
#20 0x553677 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned  
long long) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194:12  
#21 0x5529a3 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,  
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139:5  
#22 0x5529a3 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,  
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88:20  
#23 0x53def3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned  
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816:20  
#24 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&  
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14  
#25 0x5746a6 in AP4_DrefAtom::AP4_DrefAtom(unsigned int, unsigned char, unsigned int,  
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4DrefAtom.cpp:84:16  
#26 0x573f60 in AP4_DrefAtom::Create(unsigned int, AP4_ByteStream&, AP4_AtomFactory&)  
/benchmark/Bento4/Source/C++/Core/Ap4DrefAtom.cpp:50:16  
#27 0x53ed78 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned  
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:580:20  
#28 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&  
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14  
#29 0x553677 in AP4_ContainerAtom::ReadChildren(AP4_AtomFactory&, AP4_ByteStream&, unsigned  
long long) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:194:12  
#30 0x5529a3 in AP4_ContainerAtom::AP4_ContainerAtom(unsigned int, unsigned long long, bool,  
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:139:5  
#31 0x5529a3 in AP4_ContainerAtom::Create(unsigned int, unsigned long long, bool, bool,  
AP4_ByteStream&, AP4_AtomFactory&) /benchmark/Bento4/Source/C++/Core/Ap4ContainerAtom.cpp:88:20  
#32 0x53def3 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned int, unsigned  
int, unsigned long long, AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:816:20  
#33 0x53bbf1 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, unsigned long long&  
AP4_Atom*&) /benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:234:14  
#34 0x53b237 in AP4_AtomFactory::CreateAtomFromStream(AP4_ByteStream&, AP4_Atom*&)
```

/benchmark/Bento4/Source/C++/Core/Ap4AtomFactory.cpp:154:12

SUMMARY: AddressSanitizer: heap-buffer-overflow /dependence/llvm11/llvm-11.0.0.src/projects/compiler-rt/lib/asan/./sanitizer_common/sanitizer_common_interceptors.inc:1027:16 in __interceptor_fread.part.0

Shadow bytes around the buggy address:

```
0x0c047fff7fd0: 00 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 00
0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c047fff8000: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
0x0c047fff8010: fa fa 00 fa fa fa fd fa fa fa fd fa fa fa 01 fa
=>0x0c047fff8020: fa fa fd fa fa fa fd fa fa fa 01 fa fa fa[01]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
0x0c047fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8070: 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

==1448318==ABORTING

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

