New issue

Jump to bottom

there are some vulnerabilities in binary mp4split #756

Open **yuhanghuang** opened this issue on Sep 14 · 2 comments

yuhanghuang commented on Sep 14

Hello, I use fuzzer to test bianry mp4split, and found some vulnerabilities,the following is the details.

Bug1

```
root@c511e4bf49bc:/mp4split/mp4split# ./mp4split
FishFuzz/crashes/id:000000,sig:06,src:000011,op:flip1,pos:31240,1216870
=================================================================
==2589461==ERROR: AddressSanitizer: global-buffer-overflow on address 0x000000cfdb21 at pc
0x0000009a6c6c bp 0x7ffec6ff0d60 sp 0x7ffec6ff0510
READ of size 237 at 0x000000cfdb21 thread T0
    #0 0x9a6c6b in __interceptor_fwrite.part.57 /llvm/llvm-project/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:1143
    #1 0x7ab8fa in AP4_StdcFileByteStream::WritePartial(void const*, unsigned int, unsigned int&)
(/mp4split/mp4split/mp4split+0x7ab8fa)
    #2 0x471cf7 in AP4_ByteStream::Write(void const*, unsigned int)
(/mp4split/mp4split/mp4split+0x471cf7)
    #3 0x4d1be1 in AP4_HdlrAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x4d1be1)
    #4 0x41378f in AP4_AtomListWriter::Action(AP4_Atom*) const
(/mp4split/mp4split/mp4split+0x41378f)
    #5 0x483213 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x483213)
    #6 0x41378f in AP4_AtomListWriter::Action(AP4_Atom*) const
(/mp4split/mp4split/mp4split+0x41378f)
    #7 0x483213 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x483213)
    #8 0x41378f in AP4_AtomListWriter::Action(AP4_Atom*) const
(/mp4split/mp4split/mp4split+0x41378f)
    #9 0x483213 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x483213)
    #10 0x40d872 in main (/mp4split/mp4split/mp4split+0x40d872)
    #11 0x7f7ce8910c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #12 0x407689 in _start (/mp4split/mp4split/mp4split+0x407689)
```

```
0x000000cfdb21 is located 63 bytes to the left of global variable 'AP4_GlobalOptions::g_Entries'
defined in '/Bento4-1.5.1-629/Source/C++/Core/Ap4Utils.cpp:37:56' (0xcfdb60) of size 8
0x000000cfdb21 is located 0 bytes to the right of global variable 'AP4_String::EmptyString'
defined in '/Bento4-1.5.1-629/Source/C++/Core/Ap4String.cpp:39:18' (0xcfdb20) of size 1
  'AP4_String::EmptyString' is ascii string ''
SUMMARY: AddressSanitizer: global-buffer-overflow /llvm/llvm-project/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:1143 in
__interceptor_fwrite.part.57
Shadow bytes around the buggy address:
  0x000080197b10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x000080197b20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f9
  0x000080197b30: f9 f9 f9 f9 00 00 00 f9 f9 f9 f9 f9 00 00 00 f9
  0x000080197b40: f9 f9 f9 f9 00 00 00 00 00 00 00 00 f9 f9 f9
  0x000080197b50: f9 f9 f9 f9 00 00 00 00 00 00 00 00 f9 f9 f9
=>0x000080197b60: f9 f9 f9 f9[01]f9 f9 f9 f9 f9 f9 f9 00 f9 f9 f9
  0x000080197b70: f9 f9 f9 f9 00 00 00 f9 f9 f9 f9 f9 00 00 00 00
  0x000080197b80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x000080197b90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x000080197ba0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x000080197bb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==2589461==ABORTING
```

Bug2

```
root@c511e4bf49bc:/mp4split/mp4split# ./mp4split
FishFuzz/crashes/id:000001,sig:06,src:000011,op:flip1,pos:31415,1226899
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2659777==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000096b50a bp
0x7ffda4354030 sp 0x7ffda4353e70 T0)
==2659777==The signal is caused by a READ memory access.
==2659777==Hint: address points to the zero page.
```

```
    #0 0x96b50a in AP4_DescriptorListWriter::Action(AP4_Descriptor*) const
(/mp4split/mp4split/mp4split+0x96b50a)
    #1 0x88e625 in AP4_EsDescriptor::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x88e625)
    #2 0x896a7f in AP4_Expandable::Write(AP4_ByteStream&) (/mp4split/mp4split/mp4split+0x896a7f)
    #3 0x4bdbcd in AP4_EsdsAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x4bdbcd)
    #4 0x41378f in AP4_AtomListWriter::Action(AP4_Atom*) const
(/mp4split/mp4split/mp4split+0x41378f)
    #5 0x61dbf8 in AP4_SampleEntry::Write(AP4_ByteStream&) (/mp4split/mp4split/mp4split+0x61dbf8)
    #6 0x41378f in AP4_AtomListWriter::Action(AP4_Atom*) const
(/mp4split/mp4split/mp4split+0x41378f)
    #7 0x676f0b in AP4_StsdAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x676f0b)
    #8 0x41378f in AP4_AtomListWriter::Action(AP4_Atom*) const
(/mp4split/mp4split/mp4split+0x41378f)
    #9 0x483213 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x483213)
    #10 0x41378f in AP4_AtomListWriter::Action(AP4_Atom*) const
(/mp4split/mp4split/mp4split+0x41378f)
    #11 0x483213 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x483213)
    #12 0x41378f in AP4_AtomListWriter::Action(AP4_Atom*) const
(/mp4split/mp4split/mp4split+0x41378f)
    #13 0x483213 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x483213)
    #14 0x41378f in AP4_AtomListWriter::Action(AP4_Atom*) const
(/mp4split/mp4split/mp4split+0x41378f)
    #15 0x483213 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x483213)
    #16 0x41378f in AP4_AtomListWriter::Action(AP4_Atom*) const
(/mp4split/mp4split/mp4split+0x41378f)
    #17 0x483213 in AP4_ContainerAtom::WriteFields(AP4_ByteStream&)
(/mp4split/mp4split/mp4split+0x483213)
    #18 0x40d872 in main (/mp4split/mp4split/mp4split+0x40d872)
    #19 0x7f1636a2cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #20 0x407689 in _start (/mp4split/mp4split/mp4split+0x407689)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/mp4split/mp4split/mp4split+0x96b50a) in
AP4_DescriptorListWriter::Action(AP4_Descriptor*) const
==2659777==ABORTING
```

poc

crash.zip

environment

Ubuntu 18.04(docker)

credit

Yuhang Huang (NCNIPC of China)
Han Zheng (NCNIPC of China, Hexhive)

Thansk for your time!

barbibulle commented on Sep 18 Contributor

Which version of the software are you using? This does not seem to be affecting the last commit on the master branch.

yuhanghuang commented on Sep 19 Author

> Which version of the software are you using? This does not seem to be affecting the last commit on the master branch.
> Sorry, it is my problem. I use the v1.6.0-639 release version to test, and the use clang/clang++ 12.0.1 to compile the project in Ubuntu 18.04 operation system . While in the latest version,the problem has been fixed. Since the similar issues have not been comitted, I am trying to do more tests to make the issue can be reproduced in the latest commit version.
> Thanks for your reply!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants