MediaInfo Bugs

A unified display of relevant technical and tag data for A/V files

Brought to you by: guillaumeroques, zenitram

#1127 an off by one vulnerability when parsing MpegPs file format

Milestone: Crash **Status:** closed-fixed **Owner:** Jerome Martinez **Labels:** None
Priority: 5
Updated: 2020-08-31 **Created:** 2020-06-30 **Creator:** casperslei **Private:** No

There is an off by one vulnerability when parsing MpegPs file format.

ASAN output

```
=================================================================
==114347==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffecf740d58 at pc 0x
READ of size 8 at 0x7ffecf740d58 thread T0
    #0 0x122cbd8 in MediaInfoLib::File_MpegPs::Streams_Fill_PerStream(unsigned long, MediaI
    #1 0x1228c53 in MediaInfoLib::File_MpegPs::Streams_Fill() /home/casper/mi/tmp/MediaInfo
    #2 0x1b10465 in MediaInfoLib::File__Analyze::Fill(char const*) /home/casper/mi/tmp/Medi
    #3 0x1b33cea in MediaInfoLib::File__Analyze::Fill(MediaInfoLib::File__Analyze*) /home/c
    #4 0x12fbfaf in MediaInfoLib::File_MpegTs::Read_Buffer_AfterParsing() /home/casper/mi/t
    #5 0x1b03d19 in MediaInfoLib::File__Analyze::Open_Buffer_Continue_Loop() /home/casper/m
    #6 0x1afe82e in MediaInfoLib::File__Analyze::Open_Buffer_Continue(unsigned char const*,
    #7 0x6b8b2b in MediaInfoLib::MediaInfo_Internal::Open_Buffer_Continue(unsigned char con
    #8 0x17470b3 in MediaInfoLib::Reader_File::Format_Test_PerParser_Continue(MediaInfoLib:
    #9 0x1742313 in MediaInfoLib::Reader_File::Format_Test_PerParser(MediaInfoLib::MediaInf
    #10 0x173f1be in MediaInfoLib::Reader_File::Format_Test(MediaInfoLib::MediaInfo_Interna
    #11 0x6833a7 in MediaInfoLib::MediaInfo_Internal::Entry() /home/casper/mi/tmp/MediaInfo
    #12 0x656276 in MediaInfoLib::MediaInfo_Internal::Open(std::__cxx11::basic_string<wchar
    #13 0x702e73 in MediaInfoLib::MediaInfoList_Internal::Entry() /home/casper/mi/tmp/Media
    #14 0x6fef54 in MediaInfoLib::MediaInfoList_Internal::Open(std::__cxx11::basic_string<w
    #15 0x4fd14d in main /home/casper/mi/tmp/MediaInfo/Project/GNU/CLI/../../../Source/CLI/
    #16 0x7fc369c32b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-
    #17 0x426469 in _start (/home/casper/mi/afl/mediainfodbg+0x426469)

Address 0x7ffecf740d58 is located in stack of thread T0 at offset 152 in frame
    #0 0x122b31f in MediaInfoLib::File_MpegPs::Streams_Fill_PerStream(unsigned long, MediaI

  This frame has 5 object(s):
    [32, 64) 'ref.tmp.i'
    [96, 152) 'Counts' (line 335) <== Memory access at offset 152 overflows this variable
    [192, 224) 'LawRating' (line 355)
    [256, 288) 'Title' (line 358)
    [320, 352) 'ref.tmp42' (line 359)
HINT: this may be a false positive if your program uses some custom stack unwind mechanism,
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/casper/mi/tmp/MediaInfoLib/Project/G
Shadow bytes around the buggy address:
  0x100059ee0150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100059ee0160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100059ee0170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100059ee0180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100059ee0190: 00 00 00 00 00 00 00 00 f1 f1 f1 f1 f8 f8 f8 f8
=>0x100059ee01a0: f2 f2 f2 f2 00 00 00 00 00 00 00[f2]f2 f2 f2 f2
  0x100059ee01b0: f8 f8 f8 f8 f2 f2 f2 f2 f8 f8 f8 f8 f2 f2 f2 f2
  0x100059ee01c0: f8 f8 f8 f8 f3 f3 f3 f3 00 00 00 00 00 00 00 00
  0x100059ee01d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100059ee01e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100059ee01f0: f1 f1 f1 f1 f8 f8 f8 f8 f2 f2 f2 f2 f8 f8 f8 f8
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
==114347==ABORTING
```

Analysis

array `Counts` is an array with `Stream_Max` length. But code trying to access `Counts[Stream_Max]` , so off by one would occur.

code snippet in `MediaInfoLib/Source/MediaInfo/Multiple/File_MpegPs.cpp`

```
332 | //--------------------------------------------------------------------------- 333 | void
File_MpegPs::Streams_Fill_PerStream(size_t StreamID, ps_stream &Temp, kindofstream KindOfStream)
334 | { 335 | size_t Counts[Stream_Max]; 336 | for (size_t StreamKind=Stream_General+1;
StreamKind<Stream_Max; StreamKind++) 337 | Counts[StreamKind]=Count_Get((stream_t)StreamKind); 338
| 339 | //By the parser 340 | StreamKind_Last=Stream_Max; 341 | size_t Count=0; 342 | if
(!Temp.Parsers.empty() &
```

reproduce steps:

1. compile mediainfo with ASAN
2. run poc with command line `mediainfo poc.m2ts`

1 Attachments

poc.m2ts

Discussion

Luigi Baldoni - *2020-08-14*

Is this still present in 20.08 ?

Jerome Martinez - *2020-08-14*

We didn't work on that yet, but should be in next release.

Jerome Martinez - *2020-08-31*

Fixed, in next version.

Jerome Martinez - *2020-08-31*

- **status**: open --> closed-fixed
- **assigned_to**: Jerome Martinez
- **Priority**: 9 --> 5

Log in to post a comment.

SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

Team

SourceForge Headquarters
225 Broadway Suite 1600
San Diego, CA 92101
+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status

Terms Privacy Opt Out Advertise