MediaInfo Bugs

A unified display of relevant technical and tag data for A/V files
Brought to you by: guillaumeroques, zenitram

#1154 heap overflow in MediaInfoLib::File_Gxf::ChooseParser_ChannelGrouping

Milestone: Crash **Status:** closed-fixed **Owner:** Jerome Martinez **Labels:** None
Priority: 5
Updated: 2020-10-24 **Created:** 2020-10-06 **Creator:** casperslei **Private:** No

desc:
This function should check `TrackID`.

```
1574  | File__Analyze* File_Gxf::ChooseParser_ChannelGrouping(int8u TrackID)
1575  | {
1576  | #ifdef MEDIAINFO_SMPTEST0337_YES
1577  |     File_ChannelGrouping* Parser;
1578  |     if (Audio_Count%2)
1579  |     {
1580  |         if (!Streams[TrackID-1].IsChannelGrouping)
```

result:

```
=================================================================
==95136==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6260000000a6 at pc 0x00
READ of size 1 at 0x6260000000a6 thread T0
    #0 0xe6a2d8 in MediaInfoLib::File_Gxf::ChooseParser_ChannelGrouping(unsigned char) /home
    #1 0xe5c7b7 in MediaInfoLib::File_Gxf::map() /home/casper/targets/struct/mediainfo/afll
    #2 0xe558f6 in MediaInfoLib::File_Gxf::Data_Parse() /home/casper/targets/struct/mediain
    #3 0x1b1a27e in MediaInfoLib::File__Analyze::Data_Manage() /home/casper/targets/struct/
    #4 0x1b0e4ad in MediaInfoLib::File__Analyze::Buffer_Parse() /home/casper/targets/struct
    #5 0x1b03c45 in MediaInfoLib::File__Analyze::Open_Buffer_Continue_Loop() /home/casper/ta
    #6 0x1afec2e in MediaInfoLib::File__Analyze::Open_Buffer_Continue(unsigned char const*,
    #7 0x6b8bbb in MediaInfoLib::MediaInfo_Internal::Open_Buffer_Continue(unsigned char cons
    #8 0x1747173 in MediaInfoLib::Reader_File::Format_Test_PerParser_Continue(MediaInfoLib:
    #9 0x17423d3 in MediaInfoLib::Reader_File::Format_Test_PerParser(MediaInfoLib::MediaInf
    #10 0x5c5fd1 in MediaInfoLib::MediaInfo_Internal::ListFormats(std::__cxx11::basic_strin
    #11 0x173f2ef in MediaInfoLib::Reader_File::Format_Test(MediaInfoLib::MediaInfo_Interna
    #12 0x683427 in MediaInfoLib::MediaInfo_Internal::Entry() /home/casper/targets/struct/m
    #13 0x6562f6 in MediaInfoLib::MediaInfo_Internal::Open(std::__cxx11::basic_string<wchar_
    #14 0x702f03 in MediaInfoLib::MediaInfoList_Internal::Entry() /home/casper/targets/stru
    #15 0x6fefe4 in MediaInfoLib::MediaInfoList_Internal::Open(std::__cxx11::basic_string<w
    #16 0x4fd13d in fuzztest(int, char**) /home/casper/targets/struct/mediainfo/aflllvm/Medi
    #17 0x4fec3f in main /home/casper/targets/struct/mediainfo/aflllvm/MediaInfo/Project/GNU
    #18 0x7f4535ab6b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-
    #19 0x426469 in _start (/home/casper/targets/struct/mediainfo/aflllvm/fuzzrun/mediainfo

0x6260000000a6 is located 90 bytes to the left of 10752-byte region [0x626000000100,0x6260
allocated by thread T0 here:
    #0 0x4f7278 in operator new(unsigned long) /home/casper/fuzz/fuzzdeps/llvm-9.0.0.src/pr
    #1 0xe6b274 in __gnu_cxx::new_allocator<MediaInfoLib::File_Gxf::stream>::allocate(unsig
    #2 0xe6b274 in std::allocator_traits<std::allocator<MediaInfoLib::File_Gxf::stream> >::
    #3 0xe6b274 in std::_Vector_base<MediaInfoLib::File_Gxf::stream, std::allocator<MediaIn
    #4 0xe6b274 in std::vector<MediaInfoLib::File_Gxf::stream, std::allocator<MediaInfoLib:

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/casper/targets/struct/mediainfo/aflll
Shadow bytes around the buggy address:
  0x0c4c7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4c7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4c7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4c7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4c7fff8000: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c4c7fff8010: fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa fa fa
  0x0c4c7fff8020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4c7fff8030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4c7fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4c7fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4c7fff8060: 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
==95136==ABORTING
```

1 Attachments

poc

Discussion

Jerome Martinez - *2020-10-24*

- Description has changed:

Diff:

```
--- old
+++ new
@@ -1,4 +1,3 @@
 ~
  desc:
  This function should check `TrackID`.
  ```
```

- **status**: open --> closed-fixed
- **assigned_to**: Jerome Martinez

Jerome Martinez - *2020-10-24*
```

Fixed.

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