New issue

Jump to bottom

A heap-buffer-overflow in RIFF.cpp:1151 #1

○ Open **seviezhou** opened this issue on Aug 15, 2020 · 0 comments

seviezhou commented on Aug 15, 2020

The User account creation has been disabled in Bugzilla, so I have to report it here.

System info

Ubuntu x86_64, gcc (Ubuntu 5.5.0-12ubuntu1), gigextract (latest master 237fd8)

Command line

./src/tools/gigextract @@ /tmp/libgig

AddressSanitizer output

```
==80141==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60700000de40 at pc 0x0000004399ac bp 0x7ffd832c3e70 sp 0x7ffd832c3e60
READ of size 4 at 0x60700000de40 thread T0
    #0 0x4399ab in RIFF::List::GetSubList(unsigned int) /home/seviezhou/libgig/src/RIFF.cpp:1151
    #1 0x4660d6 in gig::File::LoadGroups() /home/seviezhou/libgig/src/gig.cpp:6960
    #2 0x4e360b in gig::File::LoadSamples(RIFF::progress_t*) /home/seviezhou/libgig/src/gig.cpp:6346
    #3 0x4a1774 in gig::File::GetFirstSample(RIFF::progress_t*) /home/seviezhou/libgig/src/gig.cpp:6237
    #4 0x40cd3a in ExtractSamples(gig::File*, char*, std::map<unsigned int, bool, std::less<unsigned int>, std::allocator<std::pair<unsigned int const, bool> > >*)
/home/seviezhou/libgig/src/tools/gigextract.cpp:212
    #5 0x40651c in main /home/seviezhou/libgig/src/tools/gigextract.cpp:162
    #6 0x7f9a0810d83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #7 0x4082f8 in _start (/home/seviezhou/libgig/src/tools/gigextract+0x4082f8)

0x60700000de40 is located 0 bytes to the right of 80-byte region [0x60700000ddf0,0x60700000de40)
allocated by thread T0 here:
    #0 0x7f9a092ca532 in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99532)
    #1 0x437f48 in RIFF::List::LoadSubChunks(RIFF::progress_t*) /home/seviezhou/libgig/src/RIFF.cpp:1508

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/libgig/src/RIFF.cpp:1151 RIFF::List::GetSubList(unsigned int)
Shadow bytes around the buggy address:
  0x0c0e7fff9b70: 00 00 00 00 fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c0e7fff9b80: 00 00 fa fa fa fa 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff9b90: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c0e7fff9ba0: fa fa 00 00 00 00 00 00 00 00 00 00 fa fa fa fa
  0x0c0e7fff9bb0: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa 00 00
=>0x0c0e7fff9bc0: 00 00 00 00 00 00 00 00[fa]fa fa fa 00 00 00 00
  0x0c0e7fff9bd0: 00 00 00 00 00 00 fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff9be0: 00 00 00 00 fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c0e7fff9bf0: 00 00 fa fa fa fa 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff9c00: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c0e7fff9c10: fa fa 00 00 00 00 00 00 00 00 00 00 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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==80141==ABORTING
```

POC

heap-overflow-GetSubList-RIFF-1151.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant