New issue

Jump to bottom

[BUG] heap buffer overflow in gf_utf8_wcslen, utils/utf.c:442 #2179

Closed 3 tasks done **kdsjZh** opened this issue on Apr 25 · 0 comments

kdsjZh commented on Apr 25 • edited

Thanks for reporting your issue. Please make sure these boxes are checked before submitting your issue - thank you!

- [x] I looked for a similar issue and couldn't find any.
- [x] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- [x] I give enough information for contributors to reproduce my issue (meaningful title, github labels, platform and compiler, command-line ...). I can share files anonymously with this dropbox: https://www.mediafire.com/filedrop/filedrop_hosted.php?drop=eec9e058a9486fe4e99c33021481d9e1826ca9dbc242a6cfaab0fe95da5e5d95

Detailed guidelines: http://gpac.io/2013/07/16/how-to-file-a-bug-properly/

Describe the bug

There is a heap-overflow bug in gf_utf8_wcslen, utils/utf.c:442, can be triggered via MP4Box+ ASan

Step to reproduce

./configure --enable-sanitizer && make -j$(nproc)
./MP4Box -diso poc

Sanitizer output

```
[isom] invalid tag size in Xtra !
[isom] not enough bytes in box Xtra: 4 left, reading 8 (file isomedia/box_code_base.c, line
12849), skipping box
[iso file] Box "Xtra" (start 24) has 4 extra bytes
```

```
[iso file] Read Box type 00000001 (0x00000001) at position 92 has size 0 but is not at root/file
level. Forbidden, skipping end of parent box !
[iso file] Box "moof" (start 84) has 8 extra bytes
[iso file] Movie fragment but no moov (yet) - possibly broken parsing!
[iso file] Box "vwid" (start 204) has 5 extra bytes
[iso file] Unknown top-level box type 00000B01
[iso file] Incomplete box 00000B01 - start 264 size 34164724
[iso file] Incomplete file while reading for dump - aborting parsing
=================================================================
==2183542==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000011d6 at pc
0x7f95a4f4ec68 bp 0x7ffdfa692370 sp 0x7ffdfa692360
READ of size 2 at 0x6020000011d6 thread T0
    #0 0x7f95a4f4ec67 in gf_utf8_wcslen utils/utf.c:442
    #1 0x7f95a4f4ec67 in gf_utf8_wcslen utils/utf.c:438
    #2 0x7f95a542a073 in xtra_box_dump isomedia/box_dump.c:6471
    #3 0x7f95a543161d in gf_isom_box_dump isomedia/box_funcs.c:2108
    #4 0x7f95a53f7dd9 in gf_isom_dump isomedia/box_dump.c:138
    #5 0x55aea7254fbc in dump_isom_xml /home/hzheng/real-
validate/gpac/applications/mp4box/filedump.c:2053
    #6 0x55aea7239707 in mp4boxMain /home/hzheng/real-
validate/gpac/applications/mp4box/main.c:6177
    #7 0x7f95a2a160b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x55aea7215aed in _start (/home/hzheng/real-validate/gpac/bin/gcc/MP4Box+0xa9aed)

0x6020000011d6 is located 0 bytes to the right of 6-byte region [0x6020000011d0,0x6020000011d6)
allocated by thread T0 here:
    #0 0x7f95a8767bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f95a53dc17b in xtra_box_read isomedia/box_code_base.c:12875
    #2 0x7f95a542d3c3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #3 0x7f95a542d3c3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #4 0x7f95a542e815 in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #5 0x7f95a545789c in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:373
    #6 0x7f95a545da0f in gf_isom_parse_movie_boxes isomedia/isom_intern.c:860
    #7 0x7f95a545da0f in gf_isom_open_file isomedia/isom_intern.c:980
    #8 0x55aea723f1ed in mp4boxMain /home/hzheng/real-
validate/gpac/applications/mp4box/main.c:5990
    #9 0x7f95a2a160b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-buffer-overflow utils/utf.c:442 in gf_utf8_wcslen
Shadow bytes around the buggy address:
  0x0c047fff81e0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff81f0: fa fa 00 07 fa fa 07 fa fa fa fd fa fa fa 04 fa
  0x0c047fff8200: fa fa 00 02 fa fa fd fa fa fa 00 07 fa fa 00 00
  0x0c047fff8210: fa fa 00 00 fa fa 00 fa fa fa fd fa fa fa 00 04
  0x0c047fff8220: fa fa 00 00 fa fa 00 fa fa fa 00 00 fa fa 01 fa
=>0x0c047fff8230: fa fa 06 fa fa fa 01 fa fa fa[06]fa fa fa 00 00
  0x0c047fff8240: fa fa fd fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8250: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8260: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8270: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8280: 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
==2183542==ABORTING
```

version

system: ubuntu 20.04.3 LTS
compiler: gcc 9.3.0
gpac version: latest commit `a4015fa`

Credit

Han Zheng
NCNIPC of China
Hexhive

POC

POC.zip

jeanlf closed this as completed in `915e2cb` on May 16

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant