in odf_code.c line3295 have a heap-buffer-overflow #1272

Closed **Ch111p** opened this issue on Jul 8, 2019 · 1 comment

Ch111p commented on Jul 8, 2019

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

- [✓] I looked for a similar issue and couldn't find any.
- [✓] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- [✓] 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/

in odf_code.c line3295 The check for size here may have some problems.It will cause a heap overflow.And it will resulting in gf_odf_del_ipmp_tool to free a invalid address.
Here is the asan's result:

```
[ODF] Error reading descriptor (tag 3 size 0): Invalid MPEG-4 Descriptor
=================================================================
==19708== ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602c0000ff68 at pc 0x7f448e47044d bp 0x7ffd384c3670 sp 0x7ffd384c2e30
WRITE of size 16 at 0x602c0000ff68 thread T0
    #0 0x7f448e47044c (/usr/lib/x86_64-linux-gnu/libasan.so.0.0.0+0xe44c)
    #1 0x43efa1 (/home/lcy/gpac-master/bin/gcc/MP4Box+0x43efa1)
    #2 0x56cd48 (/home/lcy/gpac-master/bin/gcc/MP4Box+0x56cd48)
    #3 0x562335 (/home/lcy/gpac-master/bin/gcc/MP4Box+0x562335)
    #4 0x56d4c7 (/home/lcy/gpac-master/bin/gcc/MP4Box+0x56d4c7)
    #5 0x6d4b48 (/home/lcy/gpac-master/bin/gcc/MP4Box+0x6d4b48)
    #6 0x51d2ab (/home/lcy/gpac-master/bin/gcc/MP4Box+0x51d2ab)
    #7 0x51d814 (/home/lcy/gpac-master/bin/gcc/MP4Box+0x51d814)
    #8 0x524cb5 (/home/lcy/gpac-master/bin/gcc/MP4Box+0x524cb5)
    #9 0x525b2e (/home/lcy/gpac-master/bin/gcc/MP4Box+0x525b2e)
    #10 0x41cb6b (/home/lcy/gpac-master/bin/gcc/MP4Box+0x41cb6b)
    #11 0x7f448d75bf44 (/lib/x86_64-linux-gnu/libc-2.19.so+0x21f44)
    #12 0x40f2fd (/home/lcy/gpac-master/bin/gcc/MP4Box+0x40f2fd)
0x602c0000ff68 is located 0 bytes to the right of 360-byte region [0x602c0000fe00,0x602c0000ff68)
allocated by thread T0 here:
    #0 0x7f448e47741a (/usr/lib/x86_64-linux-gnu/libasan.so.0.0.0+0x1541a)
    #1 0x56cb6d (/home/lcy/gpac-master/bin/gcc/MP4Box+0x56cb6d)
Shadow bytes around the buggy address:
  0x0c05ffff9f90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c05ffff9fa0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c05ffff9fb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c05ffff9fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c05ffff9fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c05ffff9fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]fa fa
  0x0c05ffff9ff0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c05ffffa000: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c05ffffa010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c05ffffa020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c05ffffa030: 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
  Heap righ 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
  ASan internal:         fe
==19708== ABORTING
```

jeanlf added a commit that referenced this issue on Jul 9, 2019

`fixed potential heap buffer overflow - cf #1272` c26b0aa

jeanlf commented on Jul 9, 2019 Contributor

should now be fixed, thanks for the report - note that this code is deactivated by default in 0.9.0

jeanlf closed this as completed on Jul 9, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants