New issue

Jump to bottom

A stack-buffer-overflow in odf_dump.c:887 #1575

Closed **seviezhou** opened this issue on Aug 14, 2020 · 0 comments

seviezhou commented on Aug 14, 2020

System info

Ubuntu x86_64, gcc (Ubuntu 5.5.0-12ubuntu1), MP4Box (latest master 2aa266)

Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" ./configure --static-mp4box

Command line

./bin/gcc/MP4Box -disox -x3d -diod -latm -keep-utc -out /dev/null @@

AddressSanitizer output

```
=================================================================
==64471==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffc9b2e916f at pc 0x562be4afcd8d bp 0x7ffc9b2e8f10 sp 0x7ffc9b2e8f00
WRITE of size 1 at 0x7ffc9b2e916f thread T0
    #0 0x562be4afcd8c in DumpRawUIConfig odf/odf_dump.c:887
    #1 0x562be4b3b57e in gf_odf_dump_dcd odf/odf_dump.c:974
    #2 0x562be4b18eb0 in gf_odf_dump_desc odf/odf_dump.c:113
    #3 0x562be4b32b81 in gf_odf_dump_esd odf/odf_dump.c:536
    #4 0x562be4b18e58 in gf_odf_dump_desc odf/odf_dump.c:111
    #5 0x562be4844bc6 in esds_box_dump isomedia/box_dump.c:1221
    #6 0x562be488d749 in gf_isom_box_dump isomedia/box_funcs.c:1923
    #7 0x562be483776a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #8 0x562be488d89c in gf_isom_box_dump_done isomedia/box_funcs.c:1930
    #9 0x562be483e636 in audio_sample_entry_box_dump isomedia/box_dump.c:750
    #10 0x562be488d749 in gf_isom_box_dump isomedia/box_funcs.c:1923
    #11 0x562be483776a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #12 0x562be488d89c in gf_isom_box_dump_done isomedia/box_funcs.c:1930
    #13 0x562be4840892 in stsd_box_dump isomedia/box_dump.c:857
    #14 0x562be488d749 in gf_isom_box_dump isomedia/box_funcs.c:1923
    #15 0x562be483776a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #16 0x562be488d89c in gf_isom_box_dump_done isomedia/box_funcs.c:1930
    #17 0x562be4839fa5 in stbl_box_dump isomedia/box_dump.c:331
    #18 0x562be488d749 in gf_isom_box_dump isomedia/box_funcs.c:1923
    #19 0x562be483776a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #20 0x562be488d89c in gf_isom_box_dump_done isomedia/box_funcs.c:1930
    #21 0x562be4844d15 in minf_box_dump isomedia/box_dump.c:1236
    #22 0x562be488d749 in gf_isom_box_dump isomedia/box_funcs.c:1923
    #23 0x562be483776a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #24 0x562be488d89c in gf_isom_box_dump_done isomedia/box_funcs.c:1930
    #25 0x562be48459a5 in mdia_box_dump isomedia/box_dump.c:1279
    #26 0x562be488d749 in gf_isom_box_dump isomedia/box_funcs.c:1923
    #27 0x562be483776a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #28 0x562be488d89c in gf_isom_box_dump_done isomedia/box_funcs.c:1930
    #29 0x562be483bf01 in trak_box_dump isomedia/box_dump.c:533
    #30 0x562be488d749 in gf_isom_box_dump isomedia/box_funcs.c:1923
    #31 0x562be483776a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #32 0x562be488d89c in gf_isom_box_dump_done isomedia/box_funcs.c:1930
    #33 0x562be4838e3e in moov_box_dump isomedia/box_dump.c:217
    #34 0x562be488d749 in gf_isom_box_dump isomedia/box_funcs.c:1923
    #35 0x562be4837aba in gf_isom_dump isomedia/box_dump.c:135
    #36 0x562be4214ce9 in dump_isom_xml /home/seviezhou/gpac/applications/mp4box/filedump.c:1670
    #37 0x562be41e5fa4 in mp4boxMain /home/seviezhou/gpac/applications/mp4box/main.c:5548
    #38 0x7f7a080ccb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #39 0x562be41c3f09 in _start (/home/seviezhou/gpac/bin/gcc/MP4Box+0x27ff09)

Address 0x7ffc9b2e916f is located in stack of thread T0 at offset 511 in frame
    #0 0x562be4af934f in DumpRawUIConfig odf/odf_dump.c:875

  This frame has 3 object(s):
    [32, 35) 'szPh'
    [96, 196) 'ind_buf'
    [256, 511) 'devName' <== Memory access at offset 511 overflows this variable
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swapcontext
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow odf/odf_dump.c:887 DumpRawUIConfig
Shadow bytes around the buggy address:
  0x10001365510: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001365520: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1
  0x10001365530: f1 f1 03 f4 f4 f4 f2 f2 f2 f2 00 00 00 00 00 00
  0x10001365540: 00 00 00 00 00 00 04 f4 f4 f4 f2 f2 f2 00 00 00
  0x10001365550: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10001365560: 00 00 00 00 00 00 00 00 00 00 00 00 00[07]f3 f3
  0x10001365570: f3 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 00
  0x10001365580: 00 00 00 00 00 00 f1 f1 f1 f1 00 00 00 00 00 00
  0x10001365590: 00 00 00 00 00 00 04 f4 f4 f4 f3 f3 f3 00 00 00
  0x100013655a0: 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 00 00
  0x100013655b0: 00 00 00 00 00 00 00 00 00 00 00 04 f4 f4 f4 f3
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
  ==64471==ABORTING
```

POC

stack-overflow-DumpRawUIConfig-odf_dump-887.zip

jeanlf closed this as completed in `71f1d75` on Sep 1, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant