New issue

Jump to bottom

A heap-buffer-overflow in box_dump.c:350 #1587

Closed seviezhou opened this issue on Sep 4, 2020 · 0 comments

seviezhou commented on Sep 4, 2020

System info

Ubuntu x86_64, gcc (Ubuntu 5.5.0-12ubuntu1), MP4Box (latest master 5a884e)

Configure

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

Command line

./bin/gcc/MP4Box -disox -ttxt -2 -dump-chap-ogg -dump-cover -drtp -bt -out /dev/null @@

AddressSanitizer output

```
=================================================================
==66502==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000e054 at pc 0x7f91d0a841d9 bp 0x7ffcd7145d60 sp 0x7ffcd71454d8
READ of size 5 at 0x60200000e054 thread T0
    #0 0x7f91d0a841d8  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x601d8)
    #1 0x7f91d0a84bbc in __interceptor_vfprintf (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x60bbc)
    #2 0x55ad61358dd0 in gf_fprintf utils/os_file.c:1512
    #3 0x55ad619271c4 in url_box_dump isomedia/box_dump.c:350
    #4 0x55ad61979ed0 in gf_isom_box_dump isomedia/box_funcs.c:1926
    #5 0x55ad6192490a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #6 0x55ad6197a057 in gf_isom_box_dump_done isomedia/box_funcs.c:1933
    #7 0x55ad6192d385 in dref_box_dump isomedia/box_dump.c:863
    #8 0x55ad61979ed0 in gf_isom_box_dump isomedia/box_funcs.c:1926
    #9 0x55ad6192490a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #10 0x55ad6197a057 in gf_isom_box_dump_done isomedia/box_funcs.c:1933
    #11 0x55ad61927135 in dinf_box_dump isomedia/box_dump.c:339
    #12 0x55ad61979ed0 in gf_isom_box_dump isomedia/box_funcs.c:1926
    #13 0x55ad6192490a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #14 0x55ad6197a057 in gf_isom_box_dump_done isomedia/box_funcs.c:1933
    #15 0x55ad61931825 in minf_box_dump isomedia/box_dump.c:1253
    #16 0x55ad61979ed0 in gf_isom_box_dump isomedia/box_funcs.c:1926
    #17 0x55ad6192490a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #18 0x55ad6197a057 in gf_isom_box_dump_done isomedia/box_funcs.c:1933
    #19 0x55ad619323a5 in mdia_box_dump isomedia/box_dump.c:1296
    #20 0x55ad61979ed0 in gf_isom_box_dump isomedia/box_funcs.c:1926
    #21 0x55ad6192490a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #22 0x55ad6197a057 in gf_isom_box_dump_done isomedia/box_funcs.c:1933
    #23 0x55ad61928bb8 in trak_box_dump isomedia/box_dump.c:550
    #24 0x55ad61979ed0 in gf_isom_box_dump isomedia/box_funcs.c:1926
    #25 0x55ad6192490a in gf_isom_box_array_dump isomedia/box_dump.c:101
    #26 0x55ad6197a057 in gf_isom_box_dump_done isomedia/box_funcs.c:1933
    #27 0x55ad61925df0 in moov_box_dump isomedia/box_dump.c:217
    #28 0x55ad61979ed0 in gf_isom_box_dump isomedia/box_funcs.c:1926
    #29 0x55ad61924c92 in gf_isom_dump isomedia/box_dump.c:135
    #30 0x55ad612fef09 in dump_isom_xml /home/seviezhou/gpac/applications/mp4box/filedump.c:1671
    #31 0x55ad612d0754 in mp4boxMain /home/seviezhou/gpac/applications/mp4box/main.c:5550
    #32 0x7f91cfa50b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #33 0x55ad612afbe9 in _start (/home/seviezhou/gpac/bin/gcc/MP4Box+0x280be9)

0x60200000e054 is located 0 bytes to the right of 4-byte region [0x60200000e050,0x60200000e054)
allocated by thread T0 here:
    #0 0x7f91d0abc612 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98612)
    #1 0x55ad62bea6a9 in url_box_read isomedia/box_code_base.c:580

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 ??
Shadow bytes around the buggy address:
  0x0c047fff9bb0: fa fa 00 fa fa fa 00 00 fa fa 00 00 fa fa 02 fa
  0x0c047fff9bc0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff9bd0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff9be0: fa fa 00 00 fa fa 00 05 fa fa 00 00 fa fa 00 00
  0x0c047fff9bf0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
=>0x0c047fff9c00: fa fa 00 fa fa fa 00 00 fa fa[04]fa fa fa 00 00
  0x0c047fff9c10: fa fa 00 00 fa fa 00 05 fa fa 00 00 fa fa 00 00
  0x0c047fff9c20: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff9c30: fa fa 00 00 fa fa 00 00 fa fa fd fa fa fa 00 fa
  0x0c047fff9c40: fa fa 00 00 fa fa 00 00 fa fa 00 07 fa fa fd fa
  0x0c047fff9c50: fa fa 00 02 fa fa 04 fa fa fa fd fa fa fa 07 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
==66502==ABORTING
```

POC

heap-overflow-url_box_dump-box_dump-350.zip

jeanlf closed this as completed in `388ecce` on Sep 7, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant