[security]heap buffer overflow in MP4Box URL_GetProtocolType #1766

Closed **5n1p3r0010** opened this issue on Apr 29, 2021 · 0 comments

5n1p3r0010 commented on Apr 29, 2021

Hi,

There is a heap buffer overflow issue in gpac MP4Box URL_GetProtocolType,this can reproduce on the lattest commit.

Steps To Reproduce

build:

```
CC=gcc CXX=g++ CFLAGS="-fsanitize=address" CXXFLAGS="-fsanitize=address" LDFLAGS="-fsanitize=address" ./configure --enable-debug
make
```

run as:

```
MP4Box -info <poc>
```

shows the following log:

```
=================================================================
==3138234==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000001114 at pc 0x7f6ae63b5235 bp 0x7fff377f4c50 sp 0x7fff377f43f8
READ of size 5 at 0x602000001114 thread T0
    #0 0x7f6ae63b5234  (/lib/x86_64-linux-gnu/libasan.so.5+0x57234)
    #1 0x7f6ae6437c10 in strstr (/lib/x86_64-linux-gnu/libasan.so.5+0xd9c10)
    #2 0x7f6ae5a3f281 in URL_GetProtocolType utils/url.c:78
    #3 0x7f6ae5a3f2f2 in gf_url_is_local utils/url.c:92
    #4 0x7f6ae5c3d80b in gf_isom_datamap_new isomedia/data_map.c:150
    #5 0x7f6ae5c7658e in Media_CheckDataEntry isomedia/media.c:693
    #6 0x7f6ae5c4bd84 in gf_isom_check_data_reference isomedia/isom_read.c:1619
    #7 0x560c005bba74 in DumpTrackInfo /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:2388
    #8 0x560c005c223c in DumpMovieInfo /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:3590
    #9 0x560c005af8f5 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5904
    #10 0x560c005b1653 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6335
    #11 0x7f6ae57c40b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #12 0x560c0059d2ad in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x182ad)

0x602000001114 is located 0 bytes to the right of 4-byte region [0x602000001110,0x602000001114)
allocated by thread T0 here:
    #0 0x7f6ae646bbc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f6ae5a3f0f0 in gf_malloc utils/alloc.c:150
    #2 0x7f6ae5bef103 in unkn_box_read isomedia/box_code_base.c:760
    #3 0x7f6ae5c3c444 in gf_isom_box_read isomedia/box_funcs.c:1808
    #4 0x7f6ae5c3acdc in gf_isom_box_parse_ex isomedia/box_funcs.c:265
    #5 0x7f6ae5c3bf48 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1705
    #6 0x7f6ae5c3b268 in gf_isom_box_array_read isomedia/box_funcs.c:387
    #7 0x7f6ae5befba5 in dref_box_read isomedia/box_code_base.c:1022
    #8 0x7f6ae5c3c444 in gf_isom_box_read isomedia/box_funcs.c:1808
    #9 0x7f6ae5c3acdc in gf_isom_box_parse_ex isomedia/box_funcs.c:265
    #10 0x7f6ae5c3bf48 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1705
    #11 0x7f6ae5c3b268 in gf_isom_box_array_read isomedia/box_funcs.c:387
    #12 0x7f6ae5bef990 in dinf_box_read isomedia/box_code_base.c:975
    #13 0x7f6ae5c3c444 in gf_isom_box_read isomedia/box_funcs.c:1808
    #14 0x7f6ae5c3acdc in gf_isom_box_parse_ex isomedia/box_funcs.c:265
    #15 0x7f6ae5c3bf48 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1705
    #16 0x7f6ae5c3b268 in gf_isom_box_array_read isomedia/box_funcs.c:387
    #17 0x7f6ae5bf719e in minf_box_read isomedia/box_code_base.c:3494
    #18 0x7f6ae5c3c444 in gf_isom_box_read isomedia/box_funcs.c:1808
    #19 0x7f6ae5c3acdc in gf_isom_box_parse_ex isomedia/box_funcs.c:265
    #20 0x7f6ae5c3bf48 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1705
    #21 0x7f6ae5c3b268 in gf_isom_box_array_read isomedia/box_funcs.c:387
    #22 0x7f6ae5bf5acb in mdia_box_read isomedia/box_code_base.c:3049
    #23 0x7f6ae5c3c444 in gf_isom_box_read isomedia/box_funcs.c:1808
    #24 0x7f6ae5c3acdc in gf_isom_box_parse_ex isomedia/box_funcs.c:265
    #25 0x7f6ae5c3bf48 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1705
    #26 0x7f6ae5c3b268 in gf_isom_box_array_read isomedia/box_funcs.c:387
    #27 0x7f6ae5c04a53 in trak_box_read isomedia/box_code_base.c:6688
    #28 0x7f6ae5c3c444 in gf_isom_box_read isomedia/box_funcs.c:1808
    #29 0x7f6ae5c3acdc in gf_isom_box_parse_ex isomedia/box_funcs.c:265

SUMMARY: AddressSanitizer: heap-buffer-overflow (/lib/x86_64-linux-gnu/libasan.so.5+0x57234)
Shadow bytes around the buggy address:
  0x0c047fff81d0: fa fa fd fa fa fa 04 fa fa fa 00 02 fa fa fd fa
  0x0c047fff81e0: fa fa 00 07 fa fa 00 00 fa fa 00 00 fa fa 00 fa
  0x0c047fff81f0: fa fa fd fa fa fa 00 04 fa fa 00 00 fa fa 00 04
  0x0c047fff8200: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8210: fa fa 00 00 fa fa 00 00 fa fa 00 05 fa fa 00 00
=>0x0c047fff8220: fa fa[04]fa fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8230: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8240: fa fa 00 00 fa fa 02 fa fa fa 00 00 fa fa 00 00
  0x0c047fff8250: fa fa 00 fa fa fa 04 fa fa fa 00 00 fa fa 00 00
  0x0c047fff8260: fa fa 01 fa fa fa 00 00 fa fa 00 06 fa fa 00 00
  0x0c047fff8270: fa fa 00 00 fa fa 00 00 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
  ==3138234==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
heap-overflow_URL_GetProtocolType.zip

jeanlf closed this as completed in `328def7` on Apr 30, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant