New issue

Jump to bottom

Heap-based Buffer Overflow #2061

Closed **rbouqueau** opened this issue on Jan 21 · 0 comments

rbouqueau commented on Jan 21 Contributor

```
Proof of Concept

Version:

MP4Box - GPAC version 1.1.0-DEV-rev1646-gddd7990bb-master
(c) 2000-2022 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io

Please cite our work in your research:
        GPAC Filters: https://doi.org/10.1145/3339825.3394929
        GPAC: https://doi.org/10.1145/1291233.1291452

GPAC Configuration: --prefix=/home/aidai/fuzzing/gpac/
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SOCK_UN GPAC_MINIMAL_ODF
GPAC_HAS_QJS GPAC_HAS_LINUX_DVB  GPAC_DISABLE_3D

System information Ubuntu 20.04 focal, AMD EPYC 7742 64-Core @ 16x 2.25GHz

poc

base64 poc
//7/AGUKCio=

command:

./MP4Box -info poc

Result

=================================================================
==1529455==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000001a1a at pc
0x00000043e343 bp 0x7ffeafafa9a0 sp 0x7ffeafafa158
READ of size 11 at 0x602000001a1a thread T0
    #0 0x43e342 in StrstrCheck(void*, char*, char const*, char const*)
(/home/aidai/fuzzing/gpac/gpac-asan/bin/gcc/MP4Box+0x43e342)
    #1 0x43e171 in strstr (/home/aidai/fuzzing/gpac/gpac-asan/bin/gcc/MP4Box+0x43e171)
    #2 0x7f61341e32d7 in ctxload_probe_data /home/aidai/fuzzing/gpac/gpac-
asan/src/filters/load_bt_xmt.c:837:6
```

```
    #3 0x7f6134037b52 in gf_filter_pid_raw_new /home/aidai/fuzzing/gpac/gpac-
asan/src/filter_core/filter.c:3777:13
    #4 0x7f6134153a31 in filein_process /home/aidai/fuzzing/gpac/gpac-
asan/src/filters/in_file.c:481:7
    #5 0x7f6134030e3a in gf_filter_process_task /home/aidai/fuzzing/gpac/gpac-
asan/src/filter_core/filter.c:2515:7
    #6 0x7f613401015f in gf_fs_thread_proc /home/aidai/fuzzing/gpac/gpac-
asan/src/filter_core/filter_session.c:1756:3
    #7 0x7f613400de3e in gf_fs_run /home/aidai/fuzzing/gpac/gpac-
asan/src/filter_core/filter_session.c:2000:2
    #8 0x7f6133c4d27e in gf_media_import /home/aidai/fuzzing/gpac/gpac-
asan/src/media_tools/media_import.c:1218:3
    #9 0x524fe4 in convert_file_info /home/aidai/fuzzing/gpac/gpac-
asan/applications/mp4box/fileimport.c:128:6
    #10 0x4f45c2 in mp4boxMain /home/aidai/fuzzing/gpac/gpac-
asan/applications/mp4box/main.c:6063:6
    #11 0x7f61332740b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #12 0x429b7d in _start (/home/aidai/fuzzing/gpac/gpac-asan/bin/gcc/MP4Box+0x429b7d)

0x602000001a1a is located 0 bytes to the right of 10-byte region [0x602000001a10,0x602000001a1a)
allocated by thread T0 here:
    #0 0x4a22bd in malloc (/home/aidai/fuzzing/gpac/gpac-asan/bin/gcc/MP4Box+0x4a22bd)
    #1 0x7f613372a4fb in gf_utf_get_utf8_string_from_bom /home/aidai/fuzzing/gpac/gpac-
asan/src/utils/utf.c:680:14

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/aidai/fuzzing/gpac/gpac-
asan/bin/gcc/MP4Box+0x43e342) in StrstrCheck(void*, char*, char const*, char const*)
Shadow bytes around the buggy address:
  0x0c047fff82f0: fa fa 00 00 fa fa 04 fa fa fa 04 fa fa fa 00 00
  0x0c047fff8300: fa fa 00 00 fa fa 04 fa fa fa 00 00 fa fa 06 fa
  0x0c047fff8310: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8320: fa fa 00 00 fa fa fd fa fa fa 00 00 fa fa 00 00
  0x0c047fff8330: fa fa 04 fa fa fa 04 fa fa fa 04 fa fa fa fd fd
=>0x0c047fff8340: fa fa 00[02]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8350: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8360: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8370: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8380: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8390: 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
==1529455==ABORTING
```

 **jeanlf** closed this as completed in 96699aa on Jan 21

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant