New issue

Jump to bottom

System abort (Core dumped) caused by buffer overflow using MP4Box in gf_text_get_utf8_line #1897

Closed 3 tasks done **5hadowblad3** opened this issue on Aug 26, 2021 · 0 comments

5hadowblad3 commented on Aug 26, 2021

- [x] I looked for a similar issue and couldn't find any.
- [x] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- [x] I give enough information for contributors to reproduce my issue (meaningful title, github labels, platform and compiler, command-line ...).

Hi, there.

There is a buffer overflow in gf_text_get_utf8_line, in commit `592ba26` that results in system abort (core dumped).

Here is my environment, compiler info and gpac version:

```
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.6 LTS
Release:        16.04
Codename:       xenial
gcc: 5.4.0

MP4Box - GPAC version 1.1.0-DEV-rev1170-g592ba26-master
(c) 2000-2021 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io
        MINI build (encoders, decoders, audio and video output disabled)

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: --static-bin --enable-debug
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_SOCK_UN GPAC_MINIMAL_ODF GPAC_HAS_QJS GPAC_HAS_FREETYPE GPAC_HAS_JPEG GPAC_HAS_PNG  GPAC_DISABLE_3D
```

To reproduce, run

```
./MP4Box -info poc
```

POC:
poc.zip
(unzip first)

This is the output of the program:

```
*** stack smashing detected ***: <unknown> terminated
Aborted (core dumped)
```

Here is the trace reported by gdb (the stack is smashed):

```
Stopped reason: SIGABRT
gef➤  bt
#0  0x0000000001f15d08 in raise ()
#1  0x0000000001f15f3a in abort ()
#2  0x0000000001f24ed6 in __libc_message ()
#3  0x0000000001f70a92 in __fortify_fail ()
#4  0x0000000001f70a3e in __stack_chk_fail ()
#5  0x0000000000127f3ad in gf_text_get_utf8_line (szLine=<optimized out>, lineSize=<optimized out>, txt_in=<optimized out>, unicode_type=0x0) at
/mnt/data/playground/gpac/src/filters/load_text.c:337
#6  0xc2657485c3a5c37e in ?? ()
#7  0xbcc3739fc3314583 in ?? ()
#8  0x0748654e86c3aac3 in ?? ()
....
#14 0x609ec3a0c3a7c26e in ?? ()
#15 0x11bdcd643758a5c3 in ?? ()
#16 0x00000000009ac35e in gf_isom_load_extra_boxes (movie=0xc53f89c4114aacc2, moov_boxes=<optimized out>, moov_boxes_size=<optimized out>, udta_only=(unknown: 2747429506)) at
/mnt/data/playground/gpac/src/isomedia/isom_write.c:615
#17 0x0000000000000000 in ?? ()
```

5hadowblad3 changed the title ~~System abort (Core dump) caused by buffer overflow using MP4Box in gf_text_get_utf8_line~~ System abort (Core dumped) caused by buffer overflow using MP4Box in gf_text_get_utf8_line on Aug 27, 2021

jeanlf closed this as completed in `30ac5e5` on Aug 30, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant