New issue

Jump to bottom

Signed integer overflow #2067

Closed **AAArdu** opened this issue on Jan 26 · 1 comment

AAArdu commented on Jan 26

Description

There are some signed-integer-overflow caused runtime error and are detected by UndefinedBehaviorSanitizer

System info

```
Ubuntu 20.04.2 LTS
clang version 12.0.0-++20210402082642+04ba60cfe598-1~exp1~20210402063359.71
MP4Box - GPAC version 1.1.0-DEV-rev1663-g881c6a94a-master
```

Build command

```
./configure --static-mp4box --prefix=`realpath ./install` --enable-sanitizer --cc=clang --
cxx=clang++
```

Crash command

MP4Box -isma -timescale 600 -out /dev/null poc_file

Pocs

POCs

Crash output

poc_3

```
media_tools/av_parsers.c:5271:24: runtime error: signed integer overflow: 160041545 * 16 cannot be
represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior media_tools/av_parsers.c:5271:24 in
/zhengjie/collect/collec.sh: line 13:  9327 Aborted (core dumped)
```

poc_9

```
[iso file] Box "oinf" size 15 (start 0) invalid (read 18)
[iso file] Unknown top-level box type )85B691
[ODF] Error reading descriptor (tag 2 size 1): Invalid MPEG-4 Descriptor
[iso file] Box "sinf" (start 635) has 81 extra bytes
[ODF] Error reading descriptor (tag 2 size 1): Invalid MPEG-4 Descriptor
[ODF] Not enough bytes (11) to read descriptor (size=81)
[ODF] Error reading descriptor (tag 2 size 17): Invalid MPEG-4 Descriptor
[iso file] Box "stco" (start 859) has 239 extra bytes
[iso file] Box "stco" is larger than container box
[iso file] Box "stbl" size 339 (start 536) invalid (read 578)
[iso file] Unknown box type mvex in parent minf
[iso file] Unknown box type moov in parent minf
[iso file] Unknown box type 00000000 in parent minf
[iso file] Unknown box type u7Fl  in parent minf
media_tools/av_parsers.c:5271:24: runtime error: signed integer overflow: 551209680 * 16 cannot be
represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior media_tools/av_parsers.c:5271:24 in
/zhengjie/collect/collec.sh: line 13: 16205 Aborted (core dumped)
```

poc_19

```
media_tools/av_parsers.c:5271:24: runtime error: signed integer overflow: 414855863 * 16 cannot be
represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior media_tools/av_parsers.c:5271:24 in
/zhengjie/collect/collec.sh: line 13: 27854 Aborted (core dumped)
```

AAArdu commented on Jan 27 — Author

Sorry for uploading the wrong POC.
Here is the true POC
poc.zip

jeanlf closed this as completed in `0cd19f4` on Jan 27

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant