New issue

Jump to bottom

AddressSanitizer: stack-overflow when processing ISOM_IOD #2216

Closed **0xdd96** opened this issue on Jul 2 · 0 comments

0xdd96 commented on Jul 2

version info:

```
root:# MP4Box -version
MP4Box - GPAC version 2.1-DEV-rev232-gfcaa01ebb-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=/path_to_build --enable-debug --enable-sanitizer
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SSL GPAC_HAS_SOCK_UN
GPAC_MINIMAL_ODF GPAC_HAS_QJS GPAC_HAS_PNG GPAC_HAS_LINUX_DVB  GPAC_DISABLE_3D
```

poc:poc
command: MP4Box -hint -out /dev/null *poc*

Here is the trace reported by ASAN:

```
root:# ./MP4Box -hint -out /dev/null poc
[ODF] Error reading descriptor (tag 4 size 14): Invalid MPEG-4 Descriptor
[iso file] Unknown box type tra7F in parent moov
[ODF] Not enough bytes (3) to read descriptor (size=93)
[ODF] Error reading descriptor (tag 3 size 34): Invalid MPEG-4 Descriptor
[iso file] Read Box "esds" (start 5507) failed (Invalid MPEG-4 Descriptor) - skipping
[ODF] Not enough bytes (3) to read descriptor (size=93)
[ODF] Error reading descriptor (tag 3 size 34): Invalid MPEG-4 Descriptor
[iso file] Unknown box type drB3f in parent dinf
[iso file] Missing dref box in dinf
[iso file] extra box maxr found in hinf, deleting
Hinting track ID 1 - Type "mp4v:mp4v" (mpeg4-generic) - BW 1393 kbps
Cannot create hinter (Invalid IsoMedia File)
Track ID 6 disabled - skipping hint
```

```
ASAN:DEADLYSIGNAL
=================================================================
==15396==ERROR: AddressSanitizer: stack-overflow on address 0x7fffff7feff8 (pc 0x7ffff6f1b64d bp
0x7ffff75d2320 sp 0x7fffff7ff000 T0)
    #0 0x7ffff6f1b64c  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x10364c)
    #1 0x7ffff6f1b0e7  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x1030e7)
    #2 0x7ffff6e40271  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x28271)
    #3 0x7ffff6ef6b0a in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb0a)
    #4 0x7ffff1cba647 in gf_malloc utils/alloc.c:150
    #5 0x7ffff269f8e6 in gf_odf_new_isom_iod odf/odf_code.c:739
    #6 0x7ffff268357e in gf_odf_create_descriptor odf/desc_private.c:77
    #7 0x7ffff2684794 in gf_odf_parse_descriptor odf/descriptors.c:88
    #8 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #9 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #10 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #11 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #12 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #13 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #14 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #15 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #16 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #17 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #18 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #19 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #20 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #21 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #22 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #23 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #24 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #25 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #26 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #27 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #28 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #29 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #30 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #31 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #32 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #33 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #34 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #35 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #36 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #37 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #38 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #39 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #40 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #41 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #42 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #43 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #44 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #45 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #46 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #47 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #48 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #49 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #50 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #51 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
```

```
#52 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#53 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#54 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#55 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#56 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#57 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#58 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#59 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#60 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#61 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#62 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#63 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#64 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#65 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#66 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#67 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#68 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#69 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#70 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#71 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#72 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#73 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#74 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#75 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#76 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#77 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#78 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#79 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#80 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#81 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#82 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#83 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#84 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#85 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#86 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#87 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#88 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#89 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#90 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#91 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#92 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#93 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#94 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#95 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#96 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#97 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#98 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#99 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#100 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#101 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#102 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#103 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#104 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#105 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#106 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#107 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
```

```
#108 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#109 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#110 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#111 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#112 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#113 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#114 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#115 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#116 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#117 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#118 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#119 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#120 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#121 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#122 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#123 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#124 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#125 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#126 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#127 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#128 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#129 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#130 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#131 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#132 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#133 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#134 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#135 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#136 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#137 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#138 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#139 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#140 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#141 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#142 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#143 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#144 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#145 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#146 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#147 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#148 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#149 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#150 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#151 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#152 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#153 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#154 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#155 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#156 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#157 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#158 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#159 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#160 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#161 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#162 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#163 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
```

```
#164 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#165 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#166 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#167 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#168 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#169 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#170 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#171 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#172 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#173 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#174 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#175 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#176 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#177 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#178 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#179 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#180 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#181 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#182 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#183 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#184 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#185 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#186 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#187 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#188 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#189 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#190 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#191 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#192 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#193 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#194 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#195 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#196 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#197 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#198 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#199 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#200 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#201 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#202 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#203 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#204 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#205 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#206 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#207 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#208 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#209 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#210 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#211 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#212 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#213 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#214 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#215 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#216 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
#217 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
#218 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
#219 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
```

```
    #220 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #221 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #222 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #223 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #224 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #225 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #226 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #227 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #228 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #229 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #230 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #231 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #232 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #233 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #234 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #235 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #236 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #237 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #238 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #239 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #240 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #241 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #242 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #243 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #244 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #245 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #246 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #247 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109
    #248 0x7ffff26a0c16 in gf_odf_read_isom_iod odf/odf_code.c:847
    #249 0x7ffff2683a29 in gf_odf_read_descriptor odf/desc_private.c:292
    #250 0x7ffff2684a45 in gf_odf_parse_descriptor odf/descriptors.c:109

SUMMARY: AddressSanitizer: stack-overflow (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x10364c)
==15396==ABORTING
```

jeanlf closed this as completed in `4e56ad7` on Jul 12

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant