#2399 closed defect (fixed)

Opened 3 months ago
Closed 3 months ago

A Division by zero occurred in the function config () of libmpcodecs/vf_scale.c

Reported by:	ylzs	Owned by:	beastd
Priority:	normal	Component:	mencoder
Version:	unspecified	Severity:	major
Keywords:		Cc:	
Blocked By:		Blocking:	
Reproduced by developer:	no	Analyzed by developer:	no

Description (last modified by ylzs) Δ

Version: SVN-r38374-13.0.1

Build command: ../configure --disable-ffmpeg_a && make (compiling with asan)

Summary of the bug: An division by zero is found in fucnction config () which affects mencoder. The attached file can reproduce this issue (ASAN-recompilation is needed).

How to reproduce:

1.Command: ./mencoder -ovc lavc -oac lavc -o /dev/null ./testcase

2.Result:

```
MEncoder SVN-r38374-13.0.1 (C) 2000-2022 MPlayer Team
success: format: 0  data: 0x0 - 0x60c
libavformat version 58.29.100 (external)
libavformat file format detected.
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fcbe8798600]overread end of atom 'colr' by 10 byt
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fcbe8798600]reached eof, corrupted STCO atom
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fcbe8798600]error reading header
LAVF_header: av_open_input_stream() failed
ISO: File Type Major Brand: Original QuickTime
Quicktime/MOV file format detected.
MOV: durmap and chunkmap sample count differ (1 vs 232)
[mov] Video stream found, -vid 0
[mov] Audio stream found, -aid 1
VIDEO:  []  224x2  0bpp  13.000 fps    0.0 kbps ( 0.0 kbyte/s)
[V] filefmt:7  fourcc:0x0  size:224x2  fps:13.000  ftime:=0.0769
libavcodec version 58.54.100 (external)
Opening video filter: [expand osd=1]
Expand: -1 x -1, -1 ; -1, osd: 1, aspect: 0.000000, round: 1
==========================================================================
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
```

```
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
```

```
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [ffmpeg] FFmpeg's libavcodec codec family
[rawvideo @ 0x7fcbe7d194c0]Invalid pixel format.
Could not open codec.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
RAW: depth 0 not supported
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
VDecoder init failed :(
Opening video decoder: [raw] RAW Uncompressed Video
Could not find matching colorspace - retrying with -vf scale...
Opening video filter: [scale]
Movie-Aspect is inf:1 - prescaling to correct movie aspect.
[swscaler @ 0x7fcbe886f000]bicubic scaler, from yuyv422 to yuv420p using MMXEXT
[swscaler @ 0x7fcbe886f000]using unscaled yuyv422 -> yuv420p special converter
AddressSanitizer:DEADLYSIGNAL
=================================================================
==24938==ERROR: AddressSanitizer: FPE on unknown address 0x55f9c11790cb (pc 0x5
    #0 0x55f9c11790cb in config /home/jlx/good_mplayer/mplayer/libmpcodecs/vf_s
    #1 0x55f9c10bb8a3 in vf_config_wrapper /home/jlx/good_mplayer/mplayer/libmp

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /home/jlx/good_mplayer/mplayer/libmpcodecs/vf_sc
==24938==ABORTING
```

3.Debugging with gdb

```
Breakpoint 1, config (vf=0x5560a56df640, width=224, height=<optimized out>, d_w
401                     d_width = vf->priv->h * d_width / d_height;
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
──────────────────────────────────────────────────────────────────────────[ REGIST
 RAX  0x1c0
 RBX  0x0
 RCX  0x400
 RDX  0x0
 RDI  0x0
 RSI  0xe0
 R8   0x0
 R9   0x7ffc5a17a3b0 —▸ 0x7f202bf1b4a0 (_IO_file_jumps) ◂— 0x0
 R10  0x4
 R11  0x246
```

```
R11  0x246
R12  0xe0
R13  0x32315659
R14  0x2
R15  0x5560a56df640 —▸ 0x5560a43f7ca0 (vf_info_scale) —▸ 0x5560a43cee8b ◂— 's
RBP  0xe0
RSP  0x7ffc5a17beb0 ◂— 0x0
RIP  0x5560a4238612 (config+1218) ◂— cdq
──────────────────────────────────────────────────────────────────────────────[ DISA
► 0x5560a4238612 <config+1218>    cdq
  0x5560a4238613 <config+1219>    idiv   ebx
   ↓
  0x5560a4238613 <config+1219>    idiv   ebx
──────────────────────────────────────────────────────────────────────────────[ SOURCE (
In file: /home/jlx/good_mplayer/mplayer/libmpcodecs/vf_scale.c
   396
   397     if(!opt_screen_size_x && !opt_screen_size_y && !(screen_size_xy >= 0
   398         // Compute new d_width and d_height, preserving aspect
   399         // while ensuring that both are >= output size in pixels.
   400         if (vf->priv->h * d_width > vf->priv->w * d_height) {
► 401                 d_width = vf->priv->h * d_width / d_height;
   402                 d_height = vf->priv->h;
   403         } else {
   404                 d_height = vf->priv->w * d_height / d_width;
   405                 d_width = vf->priv->w;
   406         }
──────────────────────────────────────────────────────────────────────────────[ STAC
00:0000│ rsp  0x7ffc5a17beb0 ◂— 0x0
01:0008│      0x7ffc5a17beb8 ◂— 0x1
02:0010│      0x7ffc5a17bec0 ◂— 0x2000000e0
03:0018│      0x7ffc5a17bec8 —▸ 0x5560a43cb59b ◂— 'Planar YV12'
04:0020│      0x7ffc5a17bed0 ◂— 0x100400000000
05:0028│      0x7ffc5a17bed8 —▸ 0x5560a56df8c0 —▸ 0x5560a56df980 —▸ 0x5560a56c
06:0030│      0x7ffc5a17bee0 ◂— 0x0
07:0038│      0x7ffc5a17bee8 ◂— 0xec39eef7e8469000
──────────────────────────────────────────────────────────────────────────────[ BACKTR
► f 0     5560a4238612 config+1218
  f 1     5560a4210cc7 vf_config_wrapper+135
  f 2     5560a420d2fb mpcodecs_config_vo+811
  f 3     5560a4207b5b init_video.constprop+555
  f 4     5560a4208305 init_best_video_codec+565
  f 5     5560a41c5254 main+8228
  f 6     7f202bd550b3 __libc_start_main+243
──────────────────────────────────────────────────────────────────────────────
```

Attachments (1)

- testcase (1.5 KB) - added by ylzs 3 months ago.

Change History (4)

comment:1 by ylzs, 3 months ago

Severity: critical → major

comment:2 by ylzs, 3 months ago

Description: modified (diff)

by ylzs, 3 months ago

Attachment: *testcase* added

comment:3 by reimar, 3 months ago

Resolution: → fixed
Status: new → closed

Probably fixed by r38390.
But I don't think this has anything to do with ASAN, and the issue is not reproducible on e.g. ARM architecture where there is no signal triggered by division by 0, so I cannot confirm if it's fixed.

Note: See TracTickets for help on using tickets.