#2401 closed defect (fixed)

Opened 3 months ago
Closed 3 months ago

A Division by zero occurred in function demux_avi_read_packet of libmpdemux/demux_avi.c

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

Description

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 play() which affects mencoder and mplayer 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

./mplayer ./testcase

2.Result:

```
MEncoder SVN-r38374-13.0.1 (C) 2000-2022 MPlayer Team
success: format: 0  data: 0x0 - 0x2aa8
libavformat version 58.29.100 (external)
AVI file format detected.
[aviheader] Video stream found, -vid 0
[aviheader] Audio stream found, -aid 1
AddressSanitizer:DEADLYSIGNAL
=================================================================
==32677==ERROR: AddressSanitizer: FPE on unknown address 0x563dfce77dc4 (pc 0x5
    #0 0x563dfce77dc4 in demux_avi_read_packet /home/jlx/good_mplayer/mplayer/l

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /home/jlx/good_mplayer/mplayer/libmpdemux/demux_
==32677==ABORTING
```

```
MPlayer SVN-r38374-9 (C) 2000-2022 MPlayer Team

Playing /home/jlx/crashes/id^%000048,sig^%08,src^%000002,time^%8657653,execs^%4
libavformat version 58.29.100 (external)
AVI file format detected.
[aviheader] Video stream found, -vid 0
[aviheader] Audio stream found, -aid 1


MPlayer interrupted by signal 8 in module: demux_open
- MPlayer crashed by bad usage of CPU/FPU/RAM.
```

```
  Recompile MPlayer with --enable-debug and make a 'gdb' backtrace and
  disassembly. Details in DOCS/HTML/en/bugreports_what.html#bugreports_crash.
- MPlayer crashed. This shouldn't happen.
  It can be a bug in the MPlayer code _or_ in your drivers _or_ in your
  gcc version. If you think it's MPlayer's fault, please read
  DOCS/HTML/en/bugreports.html and follow the instructions there. We can't and
  won't help unless you provide this information when reporting a possible bug.
```

```
Program received signal SIGFPE, Arithmetic exception.
0x00005637aa590311 in demux_avi_read_packet (demux=0x5637ac1247a0, ds=0x5637ac1
158           priv->avi_audio_pts=0;
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
──────────────────────────────────────────────────────────────[ REGISTERS ]──────
 RAX  0x14
 RBX  0x16
 RCX  0x0
 RDX  0x0
 RDI  0x5637ac1247a0 —▸ 0x5637aa7a3c20 (demuxer_desc_avi) —▸ 0x5637aa754dbc ◂-
 RSI  0x0
 R8   0x1
 R9   0x1
 R10  0x0
 R11  0x5637aa592800 (demux_open_hack_avi+240) ◂— mov    eax, dword ptr [rbx +
 R12  0x5637ac1260f0 —▸ 0x5637ac122480 ◂— 0x1062773130
 R13  0x5637ac1247a0 —▸ 0x5637aa7a3c20 (demuxer_desc_avi) —▸ 0x5637aa754dbc ◂-
 R14  0x62773130
 R15  0x15
 RBP  0x5637ac126050 ◂— 0x0
 RSP  0x7ffc013e54a0 —▸ 0x5637ac126050 ◂— 0x0
 RIP  0x5637aa590311 (demux_avi_read_packet+657) ◂— div    ecx
──────────────────────────────────────────────────────────────[ DISASM ]──────
 ► 0x5637aa590311 <demux_avi_read_packet+657>    div    ecx
    ↓
   0x5637aa590311 <demux_avi_read_packet+657>    div    ecx
```

```
──────────────────────────────────────────────────────────[ SOURCE (CODE) ]────
In file: /home/jlx/good_mplayer/mplayer/libmpdemux/demux_avi.c
   153    pts = priv->audio_block_no *
   154      (float)((sh_audio_t*)demux->audio->sh)->audio.dwScale /
   155      (float)((sh_audio_t*)demux->audio->sh)->audio.dwRate;
   156       } else
   157           pts=priv->avi_audio_pts; //+priv->pts_correction;
 ► 158       priv->avi_audio_pts=0;
   159       // update blockcount:
   160       priv->audio_block_no+=
   161  (len+priv->audio_block_size-1)/priv->audio_block_size;
   162   } else
   163   if(ds==demux->video){
──────────────────────────────────────────────────────────────[ STACK ]──────
00:0000| rsp  0x7ffc013e54a0 —▸ 0x5637ac126050 ◂— 0x0
01:0008|      0x7ffc013e54a8 ◂— 0xffffffffffffffff
02:0010|      0x7ffc013e54b0 ◂— 0x1
03:0018|      0x7ffc013e54b8 —▸ 0x5637ac122480 ◂— 0x1062773130
04:0020|      0x7ffc013e54c0 —▸ 0x5637ac1247a0 —▸ 0x5637aa7a3c20 (demuxer_desc
```

```
05:0028|       0x7ffc013e54c8 ◂— 0x15
06:0030|       0x7ffc013e54d0 —▸ 0x5637ac1260f0 —▸ 0x5637ac122480 ◂— 0x10627731
07:0038|       0x7ffc013e54d8 ◂— 0xffff00000000
──────────────────────────────────────────────────────────────[ BACKTRACE ]──────
 ▶ f 0     5637aa590311 demux_avi_read_packet+657
   f 1     5637aa591962 demux_avi_fill_buffer+1250
   f 2     5637aa584955 ds_fill_buffer+341
   f 3     5637aa584955 ds_fill_buffer+341
   f 4     5637aa592b1e demux_open_hack_avi+1038
   f 5     5637aa592b1e demux_open_hack_avi+1038
   f 6     5637aa592b1e demux_open_hack_avi+1038
   f 7     5637aa5858f3 demux_open_stream+931
──────────────────────────────────────────────────────────────────────────────
```

Attachments (1)

- testcase (10.7 KB) - added by ylzs 3 months ago.

Change History (2)

by ylzs, 3 months ago

Attachment: *testcase* added

comment:1 by reimar, 3 months ago

Resolution: → fixed
Status: new → closed

Fixed by r38386.

Note: See TracTickets for help on using tickets.