#2402 closed defect (duplicate)

Opened 3 months ago
Closed 3 months ago

A Division by zero occurred in function demux_open_avi() 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 (last modified by ylzs) ∆

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 demux_open_avi () 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:

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

Playing /home/jlx/crashes/id^%000056,sig^%08,src^%001688,time^%14273883,execs^%
libavformat version 58.29.100 (external)
AVI file format detected.
[aviheader] Video stream found, -vid 0
[aviheader] Audio stream found, -aid 1
AVI: No audio stream found -> no sound.


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.
```

```
MEncoder SVN-r38374-13.0.1 (C) 2000-2022 MPlayer Team
success: format: 0  data: 0x0 - 0x2ab4
libavformat version 58.29.100 (external)
AVI file format detected.
[aviheader] Video stream found, -vid 0
[aviheader] Audio stream found, -aid 1
```

```
AVI: No audio stream found -> no sound.
AddressSanitizer:DEADLYSIGNAL
=================================================================
==19160==ERROR: AddressSanitizer: FPE on unknown address 0x55eacc77d2e7 (pc 0x5
    #0 0x55eacc77d2e7 in demux_open_avi /home/jlx/good_mplayer/mplayer/libmpdem
    #1 0x55eacc77d2e7 in demux_open_hack_avi /home/jlx/good_mplayer/mplayer/lib

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /home/jlx/good_mplayer/mplayer/libmpdemux/demux_
==19160==ABORTING
```

```
Breakpoint 3, demux_open_avi (demuxer=<optimized out>) at libmpdemux/demux_avi.
571             asamples+=(len+priv->audio_block_size-1)/priv->audio_block_size
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
───────────────────────────────────────────────────────────────────────[ REGIST
 RAX  0x4
 RBX  0x55904d5f8d00 —▸ 0x55904d5f9410 ◂— 0xe1e1e1e1e1e1
 RCX  0x2fb
 RDX  0x4
 RDI  0x0
 RSI  0x55904d5f9440 ◂— 0x1062773130
 R8   0x1
 R9   0x0
 R10  0x55904d5f9470 ◂— 0x0
 R11  0x0
 R12  0x55904d5f73b0 —▸ 0x55904bcf5ec0 (demuxer_desc_avi) —▸ 0x55904bccffcc ◂—
 R13  0x55904d5f8c60 ◂— 0x0
 R14  0x55904d5f8d80 —▸ 0x55904d593400 ◂— 0x2fb00000000
 R15  0x0
 RBP  0x4
 RSP  0x7fff5a391720 —▸ 0x55904d593400 ◂— 0x2fb00000000
 RIP  0x55904bb55aa7 (demux_open_hack_avi+1351) ◂— lea    eax, [rax + r9 - 1]
─────────────────────────────────────────────────────────────────────────[ DISA
 ► 0x55904bb55aa7 <demux_open_hack_avi+1351>    lea    eax, [rax + r9 - 1]
   0x55904bb55aac <demux_open_hack_avi+1356>    xor    edx, edx
   0x55904bb55aae <demux_open_hack_avi+1358>    div    r9d
    ↓
   0x55904bb55aae <demux_open_hack_avi+1358>    div    r9d







───────────────────────────────────────────────────────────────────────[ SOURCE (
In file: /home/jlx/good_mplayer/mplayer/libmpdemux/demux_avi.c
   566         vsize+=len;
   567         ++vsamples;
   568       }
   569       else if(d_audio->id == id) {
   570         asize+=len;
 ► 571  asamples+=(len+priv->audio_block_size-1)/priv->audio_block_size;
   572       }
   573     }
   574     mp_msg(MSGT_DEMUX, MSGL_V,
   575            "AVI video size=%"PRId64" (%zu) audio size=%"PRId64" (%zu)\n"
   576            vsize, vsamples, asize, asamples);
─────────────────────────────────────────────────────────────────────────[ STAC
00:0000│ rsp  0x7fff5a391720 —▸ 0x55904d593400 ◂— 0x2fb00000000
01:0008│      0x7fff5a391728 —▸ 0x55904d5f9430 ◂— 0x1062773130
02:0010│      0x7fff5a391730 —▸ 0x55904d5f8c60 ◂— 0x0
03:0018│      0x7fff5a391738 ◂— 0xffffffff
04:0020│      0x7fff5a391740 ◂— 0x62773130ffffffff
```

```
04:0020│      0x7fff5a391740     0x627751301fffffff
05:0028│      0x7fff5a391748 ◂— 0x588a634aec56d900
06:0030│      0x7fff5a391750 ◂— 0xffffffff
07:0038│      0x7fff5a391758 —▸ 0x55904bcf5ec0 (demuxer_desc_avi) —▸ 0x55904bc
───────────────────────────────────────────────────────────────────────[ BACKTR
 ► f 0     55904bb55aa7 demux_open_hack_avi+1351
   f 1     55904bb55aa7 demux_open_hack_avi+1351
   f 2     55904bb48743 demux_open_stream+931

   f 3     55904bb49231 demux_open+753
   f 4     55904bac0642 main+1042
   f 5     7f7b8118c0b3 __libc_start_main+243
────────────────────────────────────────────────────────────────────────────────
```

Attachments (1)

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

Change History (3)

by ylzs, 3 months ago

Attachment: *testcase* added

comment:1 by ylzs, 3 months ago

Description: modified (diff)

comment:2 by reimar, 3 months ago

Resolution: → duplicate
Status: new → closed

Reported issue is duplicate of ~~#2401~~ but sample also shows a crash issue fixed in r38389.

Note: See TracTickets for help on using tickets.