#2396 closed defect (fixed)

Opened 3 months ago
Closed 3 months ago

A heap-buffer-overflow occurred in function mov_build_index() of libmpdemux/demux_mov.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) Δ

Version: SVN-r38374-13.0.1

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

Summary of the bug: An heap-buffer-overflow is found in fucnction mov_build_index () which affects mplayer and mencoder. The attached file can reproduce this issue (ASAN-recompilation is needed).

How to reproduce:

1.Command: ./mplayer testcase

2.Result:

```
MPlayer SVN-r38374-13.0.1 (C) 2000-2022 MPlayer Team

Playing
libavformat version 58.29.100 (external)
libavformat file format detected.
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7f665a275600]Version 22 is not implemented. Update
LAVF_header: av_open_input_stream() failed
ISO: File Type Major Brand: Original QuickTime
Quicktime/MOV file format detected.
[mov] Video stream found, -vid 0
Warning! pts=-285211648  length=2048
MOV: durmap and chunkmap sample count differ (1 vs 2)
=================================================================
==24664==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60300001458
READ of size 4 at 0x603000014580 thread T0
    #0 0x563d661312e4 in mov_build_index /home/jlx/good_mplayer/mplayer/libmpde
    #1 0x563d661312e4 in lschunks /home/jlx/good_mplayer/mplayer/libmpdemux/dem
    #2 0x563d6611c88c in mov_read_header /home/jlx/good_mplayer/mplayer/libmpde

0x603000014580 is located 0 bytes to the right of 32-byte region [0x60300001456
allocated by thread T0 here:
    #0 0x563d65d5a362 in __interceptor_calloc (/home/jlx/good_mplayer/asan_mpla
    #1 0x563d661263f0 in lschunks_intrak /home/jlx/good_mplayer/mplayer/libmpde
    #2 0x563d661263f0 in lschunks /home/jlx/good_mplayer/mplayer/libmpdemux/dem
    #3 0x563d66123576 in lschunks_intrak /home/jlx/good_mplayer/mplayer/libmpde
    #4 0x563d66123576 in lschunks /home/jlx/good_mplayer/mplayer/libmpdemux/dem
    #5 0x563d66123576 in lschunks_intrak /home/jlx/good_mplayer/mplayer/libmpde
    #6 0x563d66123576 in lschunks /home/jlx/good_mplayer/mplayer/libmpdemux/dem
    #7 0x563d66123576 in lschunks_intrak /home/jlx/good_mplayer/mplayer/libmpde
    #8 0x563d66123576 in lschunks /home/jlx/good_mplayer/mplayer/libmpdemux/dem
    #9 0x563d66124068 in lschunks /home/jlx/good_mplayer/mplayer/libmpdemux/dem
```

```
    #10 0x563d6611c88c in mov_read_header /home/jlx/good_mplayer/mplayer/libmpd

  0x0c067fffa860: 00 fa fa fa fd fd fd fd fa fa fd fd fd fd fa fa
  0x0c067fffa870: fd fd fd fd fa fa fd fd fd fd fa fa fd fd fd fd
  0x0c067fffa880: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
  0x0c067fffa890: fd fd fa fa fd fd fd fd fa fa 00 00 00 04 fa fa
  0x0c067fffa8a0: 00 00 00 fa fa fa 00 00 00 04 fa fa 00 00 00 00
=>0x0c067fffa8b0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fffa8c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fffa8d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fffa8e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fffa8f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fffa900: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==24664==ABORTING
```

Attachments (1)

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

Change History (4)

by ylzs, 3 months ago

Attachment: *testcase* added

comment:1 by ylzs, 3 months ago

Description: modified (diff)

comment:2 by ylzs, 3 months ago

Severity: critical → major

comment:3 by reimar, 3 months ago

Resolution: → fixed
Status: new → closed

Fixed by r38385.

Note: See TracTickets for help on using tickets.