Opened 3 months ago
Closed 3 months ago

#2392 closed defect (fixed)

A heap-buffer-overflow occurred in function gen_sh_video () of mplayer/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) ∆

Version: SVN-r38374-13.0.1

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

Summary of the bug: A heap-buffer-overflow read is found in fucnction gen_sh_video() which affects mplayer and mencoder. The attached file can reproduce this issue (ASAN-recompilation is needed) And this vulnerability can cause the crash of mplayer.

How to reproduce:

Command: ./mplayer testcase

Result:

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

Playing /home/jlx/crashes/testcase_2.
libavformat version 58.29.100 (external)
libavformat file format detected.
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fa0616d6600]STSC entry 2 is invalid (first=4 coun
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fa0616d6600]STSC entry 1 is invalid (first=918905
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fa0616d6600]STSC entry 0 is invalid (first=1 coun
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fa0616d6600]Invalid sample size -16777051
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fa0616d6600]error reading header
LAVF_header: av_open_input_stream() failed
Quicktime/MOV file format detected.
MOV: durmap and chunkmap sample count differ (90 vs 654)
MOV: durmap or chunkmap bigger than sample count (654 vs 90)
[mov] Video stream found, -vid 0
=================================================================
==12558==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60d00000fbf
READ of size 1 at 0x60d00000fbf3 thread T0
    #0 0x557c16d634c2 in gen_sh_video /home/jlx/good_mplayer/mplayer/libmpdemux
    #1 0x557c16d634c2 in lschunks /home/jlx/good_mplayer/mplayer/libmpdemux/dem
    #2 0x557c16d4e88c in mov_read_header /home/jlx/good_mplayer/mplayer/libmpde

Address 0x60d00000fbf3 is a wild pointer inside of access range of size 0x00000
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/jlx/good_mplayer/mplayer/
Shadow bytes around the buggy address:
  0x0c1a7fff9f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff9f30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff9f40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff9f50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff9f60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
=>0x0c1a7fff9f70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]fa
  0x0c1a7fff9f80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff9f90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff9fa0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff9fb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1a7fff9fc0: 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
==12558==ABORTING
```

Crash result:

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

Playing /home/jlx/crashes/id^%000002,sig^%06,src^%000761,time^%3561338,execs^%1
libavformat version 58.29.100 (external)
libavformat file format detected.
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fe319f34600]STSC entry 2 is invalid (first=4 coun
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fe319f34600]STSC entry 1 is invalid (first=918905
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fe319f34600]STSC entry 0 is invalid (first=1 coun
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fe319f34600]Invalid sample size -16777051
[mov,mp4,m4a,3gp,3g2,mj2 @ 0x7fe319f34600]error reading header
LAVF_header: av_open_input_stream() failed
Quicktime/MOV file format detected.
MOV: durmap and chunkmap sample count differ (90 vs 654)
MOV: durmap or chunkmap bigger than sample count (654 vs 90)
[mov] Video stream found, -vid 0


MPlayer interrupted by signal 11 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.
```

Attachments (1)

- testcase_2 (52.1 KB) - added by ylzs 3 months ago.

Change History (4)

by ylzs, 3 months ago

Attachment: *testcase_2* 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 r38384.

Note: See TracTickets for help on using tickets.