Opened 3 months ago
Closed 3 months ago

#2405 closed defect (fixed)

A heap-buffer-overflow occurred in function mp_getbits() of libmpdemux/mpeg_hdr.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 heap-buffer-overflow is found in fucnction mp_getbits() 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-r38374-13.0.1 (C) 2000-2022 MPlayer Team

Playing /home/jlx/crashes/id^%000297,sig^%06,src^%003761,time^%206342676,execs^
libavformat version 58.29.100 (external)
MPEG-PS file format detected.
MPEG: No audio stream found -> no sound.
=================================================================
==1487==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000002d98
READ of size 1 at 0x602000002d98 thread T0
    #0 0x555555d3906d in mp_getbits /home/jlx/good_mplayer/mplayer/libmpdemux/m
    #1 0x555555d3906d in read_golomb /home/jlx/good_mplayer/mplayer/libmpdemux/
    #2 0x555555d3906d in read_golomb_s /home/jlx/good_mplayer/mplayer/libmpdemu
    #3 0x555555d3906d in h264_parse_sps /home/jlx/good_mplayer/mplayer/libmpdem


0x602000002d98 is located 0 bytes to the right of 8-byte region [0x602000002d90
allocated by thread T0 here:
    #0 0x5555558971cd in malloc (/home/jlx/good_mplayer/asan_mplayer/mplayer+0x
    #1 0x555555d34e40 in h264_parse_sps /home/jlx/good_mplayer/mplayer/libmpdem

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/jlx/good_mplayer/mplayer/
Shadow bytes around the buggy address:
  0x0c047fff8560: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8570: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8580: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8590: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff85a0: fa fa 00 00 fa fa 00 00 fa fa 06 fa fa fa fd fd
=>0x0c047fff85b0: fa fa 00[fa]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff85c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff85d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff85d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff85e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff85f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8600: 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
==1487==ABORTING
```

Attachments (1)

- testcase (11.4 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: → fixed
Status: new → closed

Fixed by r38393.

Note: See TracTickets for help on using tickets.