#2398 closed defect (fixed)

Opened 3 months ago
Closed 3 months ago
Last modified 3 months ago

A heap-buffer-overflow occurred in function asf_init_audio_stream() of libmpdemux/asfheader.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 heap-buffer-overflow is found in fucnction asf_init_audio_stream() 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)
ASF file format detected.
[asfheader] Audio stream found, -aid 21
=================================================================
==6235==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x615000000261
READ of size 1 at 0x615000000261 thread T0
    #0 0x559f0c51f2c1 in asf_init_audio_stream /home/jlx/good_mplayer/mplayer/l

0x615000000261 is located 0 bytes to the right of 481-byte region [0x6150000000
allocated by thread T0 here:
    #0 0x559f0c1e01cd in malloc (/home/jlx/good_mplayer/asan_mplayer/mplayer+0x
    #1 0x559f0c51a6e0 in read_asf_header /home/jlx/good_mplayer/mplayer/libmpde

    #2 0x559f0c549e53 in demux_open_asf /home/jlx/good_mplayer/mplayer/libmpdem

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/jlx/good_mplayer/mplayer/
Shadow bytes around the buggy address:
  0x0c2a7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff8000: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff8020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff8030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2a7fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00[01]fa fa fa
  0x0c2a7fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c2a7fff8090: 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
==6235==ABORTING
```

Attachments (1)

- testcase (569 bytes) - added by ylzs 3 months ago.

Change History (4)

by ylzs, 3 months ago

Attachment: *testcase* added

comment:1 by ylzs, 3 months ago

Severity: critical → major

comment:2 by reimar, 3 months ago

Resolution: → fixed
Status: new → closed

Seems fixed by r38380.

comment:3 by reimar, 3 months ago

Minor note: When reporting this many issues it might make sense to give different priority or severity to invalid reads a short distance after the buffer vs other issue including invalid writes.
While there multiple issues here, this specific one could likely only read at most 5 bytes over the buffer, which limits its severity.

Note: See TracTickets for help on using tickets.