

#2393 closed defect (fixed)

Opened 3 months ago

Closed 3 months ago

Out-of-bound read in function read_meta_record() of mplayer/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 (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 out-of-bound read is found in fucnction read_meta_record() which affects mplayer and mencoder. The attached file can reproduce this issue And this vulnerability can cause the crash of mplayer.

How to reproduce:

1.Command: ./mplayer testcase

2.Result:

```
MPlayer SVN-r38374-9 (C) 2000-2022 MPlayer Team
Playing libavformat version 58.29.100 (external)
ASF file format detected.
[asfheader] Video stream found, -vid 1
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.
```

3.After debugging with gdb, I found the crash is caused by access to a piece of unmapped memory:

```
Program received signal SIGSEGV, Segmentation fault.
read_meta_record (buf_len=<synthetic pointer>, buf=0x55bcb7b4c52a2 <error: Cannot access memory at address 0x55bcb7b4c52a2>) at mplayer/libmpdemux/asfheader.c:242
242      dest->lang_list_index = AV_RL16(buf);
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
```

[REGISTERS]

```
RAX 0x9e000004
RBX 0x55bbdd4c529e ← 0x10000000000001
RDX 0x1a
RDI 0x55bbdd4c5284 ← 0xfda811cf5b4df869
R9 0x10
R11 0x1ce
R12 0x55bbdd4c529e
```

```

R12 0x55bc7b4c52a2
R13 0x0
R14 0x55bbdd4c51d0 ← 0x11cfa9478cabdca1
R15 0x1e1
RBP 0x62000103
RSP 0x7fff0e88d9f0 → 0x7fff0e88da00 ← 0x55bb000001ce
RIP 0x55bbdb4dde47 (read_asf_header+2935) ← movzx edx, word ptr [r12 + 4]

```

[DISASM]

```

► 0x55bbdb4dde47 <read_asf_header+2935> movzx edx, word ptr [r12 + 4]
0x55bbdb4dde4d <read_asf_header+2941> movzx r9d, word ptr [r12]
0x55bbdb4dde52 <read_asf_header+2946> movzx ecx, word ptr [r12 + 2]
0x55bbdb4dde58 <read_asf_header+2952> mov eax, dword ptr [r12 + 8]
0x55bbdb4dde5d <read_asf_header+2957> mov esi, edx
0x55bbdb4dde5f <read_asf_header+2959> lea rdi, [r12 + 0xc]
0x55bbdb4dde64 <read_asf_header+2964> sub ebp, edx
0x55bbdb4dde66 <read_asf_header+2966> js read_asf_header+3128 <read_a
↓
0x55bbdb4ddf08 <read_asf_header+3128> mov ebx, dword ptr [rsp + 0x44]
0x55bbdb4ddf0c <read_asf_header+3132> mov rax, qword ptr [rsp + 0x18]
0x55bbdb4ddf11 <read_asf_header+3137> mov rdi, qword ptr [rsp + 0x20]

```

[SOURCE (CODE)]

In file: /home/jlx/good_mplayer/mplayer/libmpdemux/asfheader.c

```

237 #define CHECKDEC(l, n) if (((l) -= (n)) < 0) return 0
238 static char* read_meta_record(ASF_meta_record_t* dest, char* buf,
239     int* buf_len)
240 {
241     CHECKDEC(*buf_len, 2 + 2 + 2 + 2 + 4);
242     dest->lang_list_index = AV_RL16(buf);
243     dest->stream_num = AV_RL16(&buf[2]);
244     dest->name_length = AV_RL16(&buf[4]);
245     dest->data_type = AV_RL16(&buf[6]);
246     dest->data_length = AV_RL32(&buf[8]);
247     buf += 2 + 2 + 2 + 2 + 4;

```

[STACK]

```

00:0000 | rsp 0x7fff0e88d9f0 → 0x7fff0e88da00 ← 0x55bb000001ce
01:0008 |      0x7fff0e88d9f8 ← 0xf775cd5000001e1
02:0010 |      0x7fff0e88da00 ← 0x55bb000001ce
03:0018 |      0x7fff0e88da08 → 0x55bbdd4c50f0 ← 0x11cf668e75b22630
04:0020 |      0x7fff0e88da10 → 0x55bbdd4c53c0 → 0x55bbdd461400 ← 0x0
05:0028 |      0x7fff0e88da18 → 0x55bbdd4c37a0 → 0x55bbdb712ce0 (demuxer_desc
06:0030 |      0x7fff0e88da20 ← 0x1
07:0038 |      0x7fff0e88da28 ← 0x55bb00000001

```

[BACKTRACE]

```

► f 0 55bbdb4dde47 read_asf_header+2935
f 1 55bbdb4dde47 read_asf_header+2935
f 2 55bbdb4dde47 read_asf_header+2935
f 3 55bbdb4e9059 demux_open_asf+57
f 4 55bbdb4e58f3 demux_open_stream+931
f 5 55bbdb4e63e1 demux_open+753
f 6 55bbdb414dcb main+4027
f 7 7f15770a80b3 __libc_start_main+243

```

```

pwndbg> p buf
$2 = 0x55bc7b4c52a2 <error: Cannot access memory at address 0x55bc7b4c52a2>

```

Attachments (1)

- [testcase](#) (668 bytes) - added by ylz 3 months ago.

Change History (6)

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

Description: modified (*diff*)

comment:3 by ylzs, 3 months ago

Description: modified (*diff*)

comment:4 by ylzs, 3 months ago

Severity: critical → major

comment:5 by reimar, 3 months ago

Resolution: → fixed

Status: new → closed

Fixed by r38382.

Note: See [TracTickets](#) for help on using tickets.