#8273 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

Segmentation fault in avpriv_copy_bits at libavcodec/bitstream.c:86

Reported by:	Suhwan	Owned by:	
Priority:	important	Component:	avformat
Version:	git-master	Keywords:	SIGSEGV
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	yes
Analyzed by developer:	yes		

Description

Summary of the bug:
There is a Segmentation fault in avpriv_copy_bits at libavcodec/bitstream.c:86
How to reproduce:

```
% ffmpeg_g -i $PoC -c copy tmp.loas

ffmpeg version N-95382-g62f4722582 Copyright (c) 2000-2019 the FFmpeg developers
built with clang version 6.0.0-1ubuntu2 (tags/RELEASE_600/final)
configuration: --cc=clang --cxx=clang++ --ld=clang --enable-debug
```

Here's log

```
Program received signal SIGSEGV, Segmentation fault.
0x0000000001cb6126 in avpriv_copy_bits (pb=<optimized out>, src=<optimized out>, l
86          put_bits(pb, bits, AV_RB16(src + 2 * words) >> (16 - bits));
(gdb) bt
#0  0x0000000001cb6126 in avpriv_copy_bits (pb=<optimized out>, src=<optimized out
#1  0x00000000015ee80f in latm_write_frame_header (s=<optimized out>, bs=<optimize
#2  latm_write_packet (s=<optimized out>, pkt=<optimized out>) at libavformat/latm
#3  0x0000000017c7515 in write_packet (s=0x9132ec0, pkt=<optimized out>) at libav
#4  0x00000000017cded6 in av_interleaved_write_frame (s=<optimized out>, pkt=0x7ff
#5  0x00000000004b5d9b in write_packet (of=<optimized out>, pkt=0x7fffffffc790, os
#6  0x00000000004a3f21 in do_streamcopy (ist=<optimized out>, ost=<optimized out>,
#7  process_input_packet (ist=<optimized out>, pkt=<optimized out>, no_eof=<optimi
#8  0x00000000004bf0a0 in process_input (file_index=<optimized out>) at fftools/ff
#9  0x000000000048d59b in transcode_step () at fftools/ffmpeg.c:4628
#10 transcode () at fftools/ffmpeg.c:4682
#11 0x0000000000487d54 in main (argc=9, argv=<optimized out>) at fftools/ffmpeg.c:
(gdb) disass $pc-32,$pc+32
Dump of assembler code from 0x1cb6106 to 0x1cb6146:
   0x0000000001cb6106 <avpriv_copy_bits+2038>:  repnz add %rax,%rdx
   0x0000000001cb610a <avpriv_copy_bits+2042>:  setb   %bl
   0x0000000001cb610d <avpriv_copy_bits+2045>:  cmp    %rsi,%rdx
   0x0000000001cb6110 <avpriv_copy_bits+2048>:  setae  %cl
   0x0000000001cb6113 <avpriv_copy_bits+2051>:  test   %ebp,%ebp
   0x0000000001cb6115 <avpriv_copy_bits+2053>:  js     0x1cb6153 <avpriv_copy_bits
   0x0000000001cb6117 <avpriv_copy_bits+2055>:  add    %rax,%r12
   0x0000000001cb611a <avpriv_copy_bits+2058>:  test   %cl,%cl
   0x0000000001cb611c <avpriv_copy_bits+2060>:  je     0x1cb615c <avpriv_copy_bits
   0x0000000001cb611e <avpriv_copy_bits+2062>:  and    $0xf,%ebp
   0x0000000001cb6121 <avpriv_copy_bits+2065>:  test   %r12,%r12
   0x0000000001cb6124 <avpriv_copy_bits+2068>:  je     0x1cb616e <avpriv_copy_bits
=> 0x0000000001cb6126 <avpriv_copy_bits+2070>:  movzwl (%r12),%eax
   0x0000000001cb612b <avpriv_copy_bits+2075>:  rol    $0x8,%ax
   0x0000000001cb612f <avpriv_copy_bits+2079>:  movzwl %ax,%edx
   0x0000000001cb6132 <avpriv_copy_bits+2082>:  mov    $0x10,%ecx
   0x0000000001cb6137 <avpriv_copy_bits+2087>:  sub    %ebp,%ecx
   0x0000000001cb6139 <avpriv_copy_bits+2089>:  shr    %cl,%edx
   0x0000000001cb613b <avpriv_copy_bits+2091>:  mov    %r15,%rdi
   0x0000000001cb613e <avpriv_copy_bits+2094>:  mov    %ebp,%esi
   0x0000000001cb6140 <avpriv_copy_bits+2096>:  add    $0x38,%rsp
   0x0000000001cb6144 <avpriv_copy_bits+2100>:  pop    %rbx
   0x0000000001cb6145 <avpriv_copy_bits+2101>:  pop    %r12
End of assembler dump.
```

Please confirm.
Thanks

Attachments (2)

- gdb-bitstream_86(21.3 KB) - added by Suhwan 3 years ago.
- PoC_bitstream_86.rm(312.7 KB) - added by Suhwan 3 years ago.
  poc

Change History (3)

by Suhwan, 3 years ago

Attachment: *gdb-bitstream_86*added

by Suhwan, 3 years ago

Attachment: *PoC_bitstream_86.rm*added

poc

comment:1 by James, 3 years ago

Analyzed by developer:	set
Component:	undetermined → avformat
Reproduced by developer:	set
Resolution:	→ fixed
Status:	new → closed

Fixed in dd01947397b98e94c3f2a79d5820aaf4594f4d3b.

Note: See TracTickets for help on using tickets.