New issue

Jump to bottom

Assert Failure in BitStream<false>::Get #70

Closed **sleicasper** opened this issue on May 18 · 1 comment

sleicasper commented on May 18

There is an assert failure in `BitStream<false>::Get` in `bitstream.hpp`. Depending on the usage of this library, e.g., running on remote server as a service, this could cause Deny of Service attack.

- reproduce steps:

1. unzip poc.zip
2. compile libjpeg with address sanitizer enabled
3. run `jpeg ./poc /dev/null`

- poc
  poc.zip

- stack trace

```
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
#1  0x00007ffff7054859 in __GI_abort () at abort.c:79
#2  0x00007ffff7054729 in __assert_fail_base (fmt=0x7ffff71ea588 "%s%s%s:%u: %s%sAssertion `%s'
failed.\n%n", assertion=0x5555558e3a60 "bits > 0 && bits <= 24", file=0x5555558e3a20
"../io/bitstream.hpp", line=172, function=<optimized out>) at assert.c:92
#3  0x00007ffff7066006 in __GI___assert_fail (assertion=0x5555558e3a60 "bits > 0 && bits <= 24",
file=0x5555558e3a20 "../io/bitstream.hpp", line=172, function=0x5555558e3c00 "ULONG
BitStream<bitstuffing>::Get(UBYTE) [with bool bitstuffing = false; ULONG = unsigned int; UBYTE =
unsigned char]") at assert.c:101
#4  0x00005555555b7f0d in BitStream<false>::Get (this=0x6140000003d8, bits=236 '\354') at
../io/bitstream.hpp:172
#5  0x000055555561d294 in LosslessScan::ParseMCU (this=0x614000000260, prev=0x7fffffffd3f0,
top=0x7fffffffd3b0) at losslessscan.cpp:382
#6  0x000055555561d928 in LosslessScan::ParseMCU (this=0x614000000260) at losslessscan.cpp:432
#7  0x0000555555651e64 in Scan::ParseMCU (this=0x60d000000130) at scan.cpp:1038
#8  0x00005555555ca6b6 in JPEG::ReadInternal (this=0x61b000000098, tags=0x7fffffffd850) at
jpeg.cpp:345
#9  0x00005555555c96b2 in JPEG::Read (this=0x61b000000098, tags=0x7fffffffd850) at jpeg.cpp:210
#10 0x00005555555aed39 in Reconstruct (infile=0x7fffffffe58b
"../../aflasan/fuzzrun/jpeg_out/default/crashes/id:000442,sig:06,src:005553,time:52219991,execs:24848
 outfile=0x7fffffffe602 "/dev/null", colortrafo=1, alpha=0x0, upsample=true) at
```

```
reconstruct.cpp:121
#11 0x000055555559ceaa in main (argc=3, argv=0x7fffffffe2c8) at main.cpp:747
```

thorfdbg commented on May 23 Owner

Thanks for reporting, this should be fixed in the 1.64 release.

thorfdbg closed this as completed on May 23

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants