

[New issue](#)[Jump to bottom](#)

Infinite loop in JPEG::ReadInternal #76

✓ Closed 0xdd96 opened this issue on Jun 26 · 1 comment

0xdd96 commented on Jun 26

version: latest commit [842c7ba](#)poc: [poc](#)

command: ./jpeg poc /dev/null

Here is the backtrace in GDB:

```
pwdbg> backtrace
#0  0x000055555558fa8a in Image::StartParseFrame (this=0x5555557433a0, io=0x555555741ad0) at image.cpp:658
#1  0x0000555555584739 in JPEG::ReadInternal (this=0x5555557414b8, tags=0x7fffffffdfcf) at jpeg.cpp:286
#2  0x00005555555843de in JPEG::Read (this=0x5555557414b8, tags=0x7fffffffdfcf) at jpeg.cpp:210
#3  0x000055555557a23e in Reconstruct (infile=0x7fffffff6cf ".../script/test-libjpeg/modify8", outfile=0x7fffffff6f1 "/dev/null", colortrafo=1, alpha=0x0, upsample=true) at reconstruct.cpp:121
#4  0x00005555555715be in main (argc=3, argv=0x7fffffff448) at main.cpp:747
#5  0x00007ffff7abf0b3 in __libc_start_main (main=0x55555556fac1 <main(int, char**)>, argc=3, argv=0x7fffffff448, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffff438) at ../csu/libc-start.c:308
#6  0x000055555556f5ee in _start ()
```

When `marker==0xffd9`, `ParseFrameHeader` will return `NULL` (line 627, `image.cpp`), which initializes `m_pCurrent` with `NULL` (line 667, `image.cpp`).

[libjpeg/codestream/image.cpp](#)

Lines 621 to 627 in 842c7ba

```
621     marker = io->GetWord();
622     switch(marker) {
623     case ByteStream::EOF:
624         JPG_THROW(MALFORMED_STREAM, "Image::ParseFrameHeader", "unexpected EOF while parsing the im
625         break;
626     case 0xffd9: // EOI
627         return NULL;
```

[libjpeg/codestream/image.cpp](#)

Lines 657 to 678 in 842c7ba

```
657     class Frame *Image::StartParseFrame(class ByteStream *io)
658     {
659         //
660         // This should only be called from the main image.
661         assert(m_pParent == NULL && m_pMaster == NULL);
662         //
663         // Check whether we have the frame header. Residual and alpha
664         // already parse that off as part of ParseTrailer().
665         if (m_bReceivedFrameHeader == false) {
666             assert(m_pTables);
667             m_pCurrent = ParseFrameHeader(io);
668             // Create the checksum if it is needed.
```

Since `m_bReceivedFrameHeader` is set to `true` after that (line 672, `image.cpp`), further calls to `StartParseFrame` will keep returning `m_pCurrent=NULL`.

[libjpeg/interface/jpeg.cpp](#)

Lines 284 to 353 in 842c7ba

```
284     while(m_bDecoding) {
285         if (m_pFrame == NULL) {
286             m_pFrame = m_pImage->StartParseFrame(m_pIOStream);
287             if (m_pFrame) {
288                 m_pDecoder->ParseTags(tags);
289                 if (stopflags & JPEGFLAG_DECODER_STOP_FRAME)
290                     return;
291             }
292         }
293     }
```

Such behavior leads to an infinite loop in `JPEG::ReadInternal`. When `m_pFrame==NULL` (line 285, `jpeg.cpp`), it will invoke `m_pImage->StartParseFrame` to initialize it (line 286, `jpeg.cpp`). Since `StartParseFrame` keeps returning `NULL` in this case, the while loop from line 284-353 cannot terminate.

thorfdbg commented on Jun 27

Owner

This was fixed in the latest release. Thank you.



thorfdbg closed this as completed on Jun 27

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

