
Subject: Re: Crash when loading some jpeg files
Posted by [pvictor](#) on Mon, 16 Jan 2023 09:09:53 GMT
[View Forum Message](#) <> [Reply to Message](#)

Well, after waiting for a while, I decided to find this bug myself.
I don't know if it is 100% correct, but it prevents crash on those unhappy images:
uppsrc/plugin/jpg/jpgupp.cpp: 384

```
- for(int diroff = Exif32(p + 4, end); diroff && begin + diroff < end; diroff = ExifDir(begin, end, diroff, BASE_IFD))  
+ for(int diroff = Exif32(p + 4, end); diroff>0 && begin + diroff < end; diroff = ExifDir(begin, end, diroff, BASE_IFD))
```

Best regards,
Victor
