Exiv2 - Bug #855

Segfault when accessing focalLength with 0.23

07 Oct 2012 04:08 - Tobias E.

Status:	Closed	**Start date:**	07 Oct 2012
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	metadata	**Estimated time:**	1.00 hour
Target version:	0.26		

Description

When trying to access the focal length in an image I get a segfault in value.hpp:1689.

I attached a minimal test program. The image that triggers this can be found in [0] (part0.jpg).

I am using libexiv2 version 0.23 from Debian sid.

[0] http://darktable.org/redmine/issues/8632

Associated revisions

Revision 4647 - 19 Oct 2016 19:27 - Robin Mills

#855 Fix submitted.

Revision 4649 - 21 Oct 2016 16:06 - Robin Mills

#855 Remove compiler signed/unsigned warning.

History

#1 - 25 Apr 2015 19:24 - Robin Mills

- Category set to metadata

- Status changed from New to Assigned

- Assignee set to Robin Mills

- Target version set to 0.25

Tobias

Thanks for reporting this and my sincere apologies for not having previously noticed this issue. We are approaching our v0.25 release and I'm working through Redmine and discovered this near the bottom of the pond.

And thank you for providing the sample code and the test image as a url on darktable's web site. v0.25 can read/write metadata over http (and other protocols). There is a fault in the test file (your trouble) and we should not be crashing under any circumstances (our trouble). Here's the evidence:

```
725 rmills@rmillsmbp:~/gnu/exiv2/trunk $ exiv2 -pv -g Focal http://darktable.org/redmine/attachments/download/251/part0.jpg
Error: Upper boundary of data for directory Photo, entry 0x920a is out of bounds: Offset = 0x000003dc, size = 8, exceeds buffer size by 6 Bytes; truncating the entry
0x920a Photo        FocalLength                 Rational    0   <---- Rational normally requires two values
0xa405 Photo        FocalLengthIn35mmFilm       Short       1   82
726 rmills@rmillsmbp:~/gnu/exiv2/trunk $
```

You can see that an error was detected in your file and I believe that's part what is wrong. None-the-less, your toFloat() code segfaults and I will investigate this.

#2 - 26 Apr 2015 22:10 - Tobias E.

I agree that the image is broken. I don't even know how it was created. Unfortunately we as programmers can't control what people do with our programs so dealing with broken files can't be avoided I guess. Anyway, thanks for looking into this. And hearing of a new release is great news. :)

#3 - 28 Apr 2015 12:47 - Robin Mills

Tobias

We had a team meeting on Sunday (April 26) and we have agreed v0.25 on May 17. I will be surprised if encounter a show-stopper.

The seg fault in toFloat() is puzzling. I encountered a similar issue in toLong this morning r3756. I'm going to put this crash on the "must fix" list for v0.25.

#4 - 09 May 2015 08:16 - Robin Mills

- Assignee changed from Robin Mills to Andreas Huggel

I'm pushing this one to Andreas who wrote this code. We're down inside templatized code and I'm not sure what's going on.

#5 - 02 Jun 2015 23:19 - Alan Pater

- Target version changed from 0.25 to 0.26

#6 - 19 Oct 2016 19:34 - Robin Mills

- Assignee changed from Andreas Huggel to Robin Mills

- % Done changed from 0 to 100

- Estimated time set to 1.00 h

I think this has already been fixed.

I've copied the file https://redmine.darktable.org/attachments/download/251/part0.jpg to test/data/exiv2-bug855.jpg and updated the test suite.

```
847 rmills@rmillsmbp:~/gnu/exiv2/trunk/build $ bin/Debug/exiv2 -vVg curl -g svn
exiv2 0.25 001900 (64 bit build)
svn=4644
curlprotocols=dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s rtsp scp sftp smtp smtps t
elnet tftp
library=/usr/local/lib/libcurl.4.dylib
848 rmills@rmillsmbp:~/gnu/exiv2/trunk/build $ bin/Debug/exiv2 -pa --grep Focal/i https://redmine.darktable.or
g/attachments/download/251/part0.jpg 2>/dev/null
Exif.Photo.FocalLength                       Rational    0
Exif.Photo.FocalLengthIn35mmFilm             Short       1  82.0 mm
849 rmills@rmillsmbp:~/gnu/exiv2/trunk/build $
```

#7 - 19 Oct 2016 19:54 - Robin Mills

- Status changed from Assigned to Closed

Files

main.cpp	519 Bytes	07 Oct 2012	Tobias E.