

## Exiv2 - Bug #1307

exiv2: tiffvisitor.cpp:1299: virtual void

Exiv2::Internal::TiffReader::visitDirectory(Exiv2::Internal::TiffDirectory\*): Assertion `tc.get()' failed.

08 Aug 2017 14:31 - Henri Salo

<b>Status:</b>	Closed	<b>Start date:</b>	08 Aug 2017
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Robin Mills	<b>% Done:</b>	100%
<b>Category:</b>	duplicate	<b>Estimated time:</b>	2.00 hours
<b>Target version:</b>	0.27		
<b>Description</b>			
Original report in here: <a href="https://bugzilla.redhat.com/show_bug.cgi?id=1475124">https://bugzilla.redhat.com/show_bug.cgi?id=1475124</a>			

### History

#### #1 - 08 Aug 2017 15:21 - Robin Mills

- Category set to duplicate
- Status changed from New to Assigned
- Assignee set to Robin Mills

Henri Salo wrote:

Original report in here: [https://bugzilla.redhat.com/show\\_bug.cgi?id=1475124](https://bugzilla.redhat.com/show_bug.cgi?id=1475124)

Can you confirm that I'm look at the correct file, please? I've unarrarred the file and have a file called POC On the "vanilla v0.26", I get:

```
715 rmills@rmillsmbp:~/gnu/exiv2/0.26 $ ls -alt ~/Google\ Drive/POC
-rwxr-xr-x 1 rmills staff 712 Jun 30 22:09 /Users/rmills/Google Drive/POC
716 rmills@rmillsmbp:~/gnu/exiv2/0.26 $ exiv2 -pa ~/Google\ Drive/POC
Assertion failed: (tc.get()), function visitDirectory, file tiffvisitor.cpp, line 1299.
Abort trap: 6
717 rmills@rmillsmbp:~/gnu/exiv2/0.26 $
```

On 'master', this was fixed a couple of months ago. I'm very surprised to be unable to find the issue report in which I dealt with this, however I'll find it and update you later today.

#### #2 - 08 Aug 2017 15:25 - Robin Mills

- Target version set to 0.27
- % Done changed from 0 to 50
- Estimated time set to 2.00 h

#### #3 - 08 Aug 2017 16:08 - Henri Salo

I reproduced this with 0.26 in my environment before posting this to here. Can't currently build after Git clone (not sure why yet, but receiving some xmpsdk related build errors). I had enabled Video and Webready support in my build for maxium efficiency for fuzzing. Are you available via IRC or email for easier communication?

#### #4 - 08 Aug 2017 16:18 - Robin Mills

I have smoke coming out my ears with the build. There are two major changes coming in Exiv2 v0.26.1

- 1) Make the Adobe XMPsdk an external library.
- 2) Support for C++11

I've got myself into trouble with Git (which I only started using in May). I'm trying to get the build/test stable again. That's my top priority.

I really would appreciate not being hammered about Fuzzing. I've agree that this will be the top priority in Exiv2 v0.27. However the two subjects above (+git support) are being targeted for v0.26.1.

I'm really puzzled by the disappearing bug report about this (something to do with my use of GitHub, I think). I just built a few minutes ago and here's what I have with your file.

```
794 rmills@rmillsmbp:~/gnu/github/exiv2 $ exiv2 -pa ~/Google\ Drive/POC
invalid type value detected in Image::printIFDStructure: 0
Exiv2 exception in print action for file /Users/rmills/Google Drive/POC:
invalid type value detected in Image::printIFDStructure
795 rmills@rmillsmbp:~/gnu/github/exiv2 $
```

#### **#5 - 08 Aug 2017 16:20 - Robin Mills**

Happy to talk on Skype, Google Plus, FaceTime or your favourite IM.

#### **#6 - 08 Aug 2017 16:54 - Robin Mills**

- Status changed from Assigned to Closed

- % Done changed from 50 to 100

I can't find the issue request about this matter (in Redmine Issues/Forum, nor GitHub Issues/PullRequests). Here's a discussion with another user in which I mention (on 2017-07-04) that I introduced errors 55 and 56 in response to a fuzzing issue. <https://github.com/Exiv2/exiv2/issues/15>

I've updated GitHub, and the build is OK on MacOS-X. I'll check Linux shortly.

Also happy to hear from you by email: [robin@clanmills.com](mailto:robin@clanmills.com) I'm marking this 100% done, however I'm not closing this as I expect you will want to continue the discussion.

#### **#7 - 29 Sep 2017 12:40 - Robin Mills**

Conversation is continued here. <https://github.com/Exiv2/exiv2/issues/57>