Exiv2 - Bug #1297

Segmentation fault in exiv2json

10 Jun 2017 09:03 - Chenghao Rong

Status:	Closed	**Start date:**	10 Jun 2017
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	samples	**Estimated time:**	3.00 hours
Target version:	0.28		

Description

The exiv2json program does not check the value of the offset element in the XResolution structure in the tif file. When the value of offset is a random value or error value, value_ vector which save Rational value structure is null. Program access value_ [0] caused Segmentation fault.

invalid type value detected in Image::printIFDStructure: 25700
Error: Upper boundary of data for directory Image, entry 0x0111 is out of bounds: Offset = 0x00000008, size = 32772, exceeds buffer size by 32350 Bytes; truncating the entry
Error: Directory Image, entry 0x0117 has invalid size 1073741825*4; skipping entry.
Warning: Directory Image, entry 0x0111: Size or data offset value not set, ignoring them.
Error: Offset of directory Image, entry 0x011a is out of bounds: Offset = 0x64000186; truncating the entry
Warning: Directory Image, entry 0x6464 has unknown Exif (TIFF) type 25700; setting type size 1.
Error: Directory Image, entry 0x6464 has invalid size 1684300900*1; skipping entry.
ASAN:SIGSEGV ===
8557ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7fee08cf2ce2 sp 0x7ffc6fd6d820 bp 0x7ffc6fd6da70 T0)
8557WARNING: Trying to symbolize code, but external symbolizer is not initialized!
#0 0x7fee08cf2ce1 (/home/lolopop/projects/exiv2-new/clang-debu/src/libexiv2.so.26+0x44cce1)
#1 0x4a422c (/home/lolopop/projects/exiv2-new/clang-debu/bin/exiv2json+0x4a422c)
#2 0x49d149 (/home/lolopop/projects/exiv2-new/clang-debu/bin/exiv2json+0x49d149)
#3 0x7fee07272f44 (/lib/x86_64-linux-gnu/libc.so.6+0x21f44)
#4 0x491adc (/home/lolopop/projects/exiv2-new/clang-debu/bin/exiv2json+0x491adc)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ??:0 ??
8557ABORTING

History

#1 - 10 Jun 2017 09:10 - Robin Mills

- Category set to samples

- Status changed from New to Assigned

- Target version changed from 0.26 to 0.28

- Estimated time set to 2.00 h

Thanks Chenghao, I have reproduced this. I'll fix this during the weekend.

#2 - 11 Jun 2017 11:28 - Robin Mills

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

- Estimated time changed from 2.00 h to 3.00 h

Fix submitted: d3c2b99

```
1211 rmills@rmillsmbp:~/gnu/git/exiv2 $ bin/exiv2json ~/Downloads/crash067
invalid type value detected in Image::printIFDStructure:  25700
Caught Exiv2 exception 'invalid type value detected in Image::printIFDStructure'
1212 rmills@rmillsmbp:~/gnu/git/exiv2 $
```

Files

crash067	430 Bytes	10 Jun 2017	Chenghao Rong
report.pdf	432 KB	10 Jun 2017	Chenghao Rong