Exiv2 - Bug #1314

it is a stack-overflow vulnerability in Exiv2::Internal::stringFormat[abi:cxx11] (in image.cpp:975)

23 Sep 2017 03:53 - Zhu Liu

Status:	Closed	**Start date:**	23 Sep 2017
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	miscellaneous	**Estimated time:**	1.00 hour
Target version:	0.27		

Description

I've submitted the vulnerability on bugzilla.redhat.com. the link is: https://bugzilla.redhat.com/show_bug.cgi?id=1494787

./exiv2 009-stack-over
ASAN:SIGSEGV ===
65094ERROR: AddressSanitizer: stack-overflow on address 0x7ffe028e0e88 (pc 0x7f1dab2e2b79 bp 0x7ffe028e1740 sp 0x7ffe028e0e90 T0)
#0 0x7f1dab2e2b78 (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x5fb78)
#1 0x7f1dab2e4145 in __interceptor_vsnprintf (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x61145)
#2 0x7f1daab94e09 in Exiv2::Internal::stringFormat[abi:cxx11](char const*, ...) /root/fuzzing/exiv2-trunk/src/image.cpp:975
#3 0x7f1daab8fc59 in Exiv2::Image::printIFDStructure(Exiv2::BasicIo&, std::ostream&, Exiv2::PrintStructureOption, unsigned int, bool, char, int) /root/fuzzing/exiv2-trunk/src/image.cpp:357
#4 0x7f1daab9097c in Exiv2::Image::printIFDStructure(Exiv2::BasicIo&, std::ostream&, Exiv2::PrintStructureOption, unsigned int, bool, char, int) /root/fuzzing/exiv2-trunk/src/image.cpp:445
#5 0x7f1daab9097c in Exiv2::Image::printIFDStructure(Exiv2::BasicIo&, std::ostream&, Exiv2::PrintStructureOption, unsigned int, bool, char, int) /root/fuzzing/exiv2-trunk/src/image.cpp:445
#6 0x7f1daab9097c in Exiv2::Image::printIFDStructure(Exiv2::BasicIo&, std::ostream&, Exiv2::PrintStructureOption, unsigned int, bool, char, int) /root/fuzzing/exiv2-trunk/src/image.cpp:445
#7 0x7f1daab9097c in Exiv2::Image::printIFDStructure(Exiv2::BasicIo&, std::ostream&, Exiv2::PrintStructureOption, unsigned int, bool, char, int) /root/fuzzing/exiv2-trunk/src/image.cpp:445
#8 0x7f1daab9097c in Exiv2::Image::printIFDStructure(Exiv2::BasicIo&, std::ostream&, Exiv2::PrintStructureOption, unsigned int, bool, char, int) /root/fuzzing/exiv2-trunk/src/image.cpp:445
#9 0x7f1daab9097c in Exiv2::Image::printIFDStructure(Exiv2::BasicIo&, std::ostream&, Exiv2::PrintStructureOption, unsigned int, bool, char, int) /root/fuzzing/exiv2-trunk/src/image.cpp:445
#10 0x7f1daab9097c in Exiv2::Image::printIFDStructure(Exiv2::BasicIo&, std::ostream&, Exiv2::PrintStructureOption, unsigned int, bool, char, int) /root/fuzzing/exiv2-trunk/src/image.cpp:445
.....
.....
.....
.....
SUMMARY: AddressSanitizer: stack-overflow ??:0 ??
65094ABORTING

History

#1 - 25 Sep 2017 19:06 - Robin Mills

- Assignee deleted (Robin Mills)

- Priority changed from Urgent to Normal

#2 - 18 Sep 2018 12:27 - Robin Mills

- Status changed from New to Closed

- Assignee set to Robin Mills

- % Done changed from 0 to 100

- Estimated time set to 1.00 h

Issue is no longer present on 'master' for Exiv2 v0.27 RC1

Normal build:

```
692 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 -pa ~/Downloads/009-stack-over.dms
Error: Directory Image: Next pointer is out of bounds; ignored.
```

```
Error: Offset of directory Image, entry 0x00fe is out of bounds: Offset = 0x00000000; truncating the entry
Error: Directory Image, entry 0x0100 has invalid size 1935897193*2; skipping entry.
Warning: Directory Image, entry 0x303e has unknown Exif (TIFF) type 12320; setting type size 1.
Error: Offset of directory Image, entry 0x0116 is out of bounds: Offset = 0x0011302a; truncating the entry
Warning: Directory Image, entry 0x0111: Strip 0 is outside of the data area; ignored.
Exif.Image.NewSubfileType                    Ifd         0
Exif.Image.BitsPerSample                     Short       4  12336 12336 12336 12336
Exif.Image.Compression                       Short       1  LZW
Exif.Image.PhotometricInterpretation         Short       1  RGB
Exif.Image.StripOffsets                      Long        1  12336
Exif.Image.Orientation                       Short       1  top, left
Exif.Image.SamplesPerPixel                   Short       1  4
Exif.Image.RowsPerStrip                      Short       0
Exif.Image.StripByteCounts                   Double      1  1.39804328609529e-76
693 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 -pR ~/Downloads/009-stack-over.dms
STRUCTURE OF TIFF FILE (MM): /Users/rmills/Downloads/009-stack-over.dms
 address |    tag                              |      type |    count |    offset | value
Exiv2 exception in print action for file /Users/rmills/Downloads/009-stack-over.dms:
invalid memory allocation request
694 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $
```

ASAN:

```
As above.
```

Files

009-stack-over	340 Bytes	23 Sep 2017	Zhu Liu