Exiv2 - Bug #1319

It is a heap-buffer-overflow in Exiv2::us2Data (types.cpp:346)

23 Sep 2017 04:15 - Zhu Liu

Status:	Closed	**Start date:**	23 Sep 2017
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	exif	**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=1494778

1. ./exiv2 004-heap-buffer-over
   invalid type value detected in Image::printIFDStructure: 250
   Error: Offset of directory Image, entry 0x00fe is out of bounds: Offset = 0x00000000; truncating the entry
   Warning: Directory Image, entry 0xfa00 has unknown Exif (TIFF) type 250; setting type size 1.
   Error: Offset of directory Image, entry 0xfa00 is out of bounds: Offset = 0x30000184; truncating the entry
   Error: Directory Photo with 8224 entries considered invalid; not read.
   ==========
   31594ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62100001661c at pc 0x7f684e7c8288 bp 0x7ffc142fd380 sp 0x7ffc142fd370
   WRITE of size 1 at 0x62100001661c thread T0
   #0 0x7f684e7c8287 in Exiv2::us2Data(unsigned char*, unsigned short, Exiv2::ByteOrder)
   /root/fuzzing/exiv2-trunk/src/types.cpp:346
   #1 0x7f684e66e268 in long Exiv2::toData<unsigned short>(unsigned char*, unsigned short, Exiv2::ByteOrder)
   /root/fuzzing/exiv2-trunk/include/exiv2/value.hpp:1450
   #2 0x7f684e67b3b7 in Exiv2::ValueType<unsigned short>::copy(unsigned char*, Exiv2::ByteOrder) const
   /root/fuzzing/exiv2-trunk/include/exiv2/value.hpp:1612
   #3 0x7f684e698aa4 in Exiv2::Exifdatum::copy(unsigned char*, Exiv2::ByteOrder) const /root/fuzzing/exiv2-trunk/src/exif.cpp:362
   #4 0x7f684e79deff in Exiv2::TiffImage::readMetadata() /root/fuzzing/exiv2-trunk/src/tiffimage.cpp:204
   #5 0x43ab02 in Action::Print::printSummary() /root/fuzzing/exiv2-trunk/src/actions.cpp:289
   #6 0x43a1af in Action::Print::run(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&)
   /root/fuzzing/exiv2-trunk/src/actions.cpp:244
   #7 0x422129 in main /root/fuzzing/exiv2-trunk/src/exiv2.cpp:170
   #8 0x7f684da1782f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
   #9 0x421af8 in _start (/usr/local/exiv2_ASAN/bin/exiv2+0x421af8)

0x62100001661c is located 0 bytes to the right of 4380-byte region [0x621000015500,0x62100001661c)
allocated by thread T0 here:
#0 0x7f684ee446b2 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x996b2)
#1 0x7f684e7c6695 in Exiv2::DataBuf::alloc(long) /root/fuzzing/exiv2-trunk/src/types.cpp:158
#2 0x7f684e79de62 in Exiv2::TiffImage::readMetadata() /root/fuzzing/exiv2-trunk/src/tiffimage.cpp:203
#3 0x43ab02 in Action::Print::printSummary() /root/fuzzing/exiv2-trunk/src/actions.cpp:289
#4 0x43a1af in Action::Print::run(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&)
/root/fuzzing/exiv2-trunk/src/actions.cpp:244
#5 0x422129 in main /root/fuzzing/exiv2-trunk/src/exiv2.cpp:170
#6 0x7f684da1782f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)

SUMMARY: AddressSanitizer: heap-buffer-overflow /root/fuzzing/exiv2-trunk/src/types.cpp:346 Exiv2::us2Data(unsigned char*, unsigned short, Exiv2::ByteOrder)
Shadow bytes around the buggy address:
0x0c427fffac70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c427fffac80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c427fffac90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c427fffaca0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c427fffacb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c427fffacc0: 00 00 00[04]fa fa fa fa fa fa fa fa fa fa fa
0x0c427fffacd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c427ffface0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c427fffacf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c427fffad00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c427fffad10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

```
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable:           00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:       fa
Heap right redzone:      fb
Freed heap region:       fd
Stack left redzone:      f1
Stack mid redzone:       f2
Stack right redzone:     f3
Stack partial redzone:   f4
Stack after return:      f5
Stack use after scope:   f8
Global redzone:          f9
Global init order:       f6
Poisoned by user:        f7
Container overflow:      fc
Array cookie:            ac
Intra object redzone:    bb
ASan internal:           fe
31594ABORTING
```

History

#1 - 25 Sep 2017 19:04 - Robin Mills

- Assignee deleted (Robin Mills)

- Priority changed from Urgent to Normal

#2 - 18 Sep 2018 12:20 - 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:

```
679 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 ~/Downloads/004-heap-buffer-over.dms
Error: Offset of directory Image, entry 0x00fe is out of bounds: Offset = 0x00000000; truncating the entry
Warning: Directory Image, entry 0xfa00 has unknown Exif (TIFF) type 250; setting type size 1.
Error: Offset of directory Image, entry 0xfa00 is out of bounds: Offset = 0x30000184; truncating the entry
Error: Directory Photo with 8224 entries considered invalid; not read.
File name       : /Users/rmills/Downloads/004-heap-buffer-over.dms
File size       : 352222 Bytes
MIME type       : image/tiff
Image size      : 17 x 12288
Camera make     :
Camera model    :
Image timestamp :
Image number    :
Exposure time   :
Aperture        :
Exposure bias   :
Flash           :
Flash bias      :
Focal length    :
Subject distance:
ISO speed       :
Exposure mode   :
Metering mode   :
Macro mode      :
Image quality   :
Exif Resolution : 17 x 12288
White balance   :
Thumbnail       : None
Copyright       :
Exif comment    :
```

```
680 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 -pR ~/Downloads/004-heap-buffer-over.dms
STRUCTURE OF TIFF FILE (MM): /Users/rmills/Downloads/004-heap-buffer-over.dms
 address |    tag                              |      type |    count |    offset | value
      10 | 0x00fe NewSubfileType               |      LONG |    42753 |         0 | 1296891946 8 1638654 26214
4 2801860608 ...
      22 | 0x0100 ImageWidth                   |     SHORT |        1 |           | 17
      34 | 0x0101 ImageLength                  |     SHORT |        1 |           | 12288
      46 | 0x0102 BitsPerSample                |     SHORT |        4 |       304 | 5424 0 29640 0
      58 | 0x0103 Compression                  |     SHORT |        1 |           | 5
      70 | 0x0106 PhotometricInterpretation    |     SHORT |        1 |           | 2
      82 | 0x0111 StripOffsets                 |      LONG |        1 |           | 12336
      94 | 0x0112 Orientation                  |     SHORT |        1 |           | 1
     106 | 0x0115 SamplesPerPixel              |     SHORT |        1 |           | 4
     118 | 0x0116 RowsPerStrip                 |     SHORT |        1 |           | 17
     130 | 0x0117 StripByteCounts              |      LONG |        1 |           | 612
     142 | 0x011a XResolution                  |  RATIONAL |        1 |       304 | 355467264/1942487040
     154 | 0x011b YResolution                  |  RATIONAL |        1 |       330 | 667696/12304
     166 | 0x011c PlanarConfiguration          |     SHORT |        1 |           | 1
     178 | 0x0128 ResolutionUnit               |     SHORT |        1 |           | 2
     190 | 0x0131 Software                     |     ASCII |       30 |       338 | Ad0be Photoshop CS3 Macin0
osh
     202 | 0x0132 DateTime                     |     ASCII |       20 |       368 | 0008006013010056040
     214 | 0x013d Predictor                    |     SHORT |        1 |           | 48
     226 | 0x0152 ExtraSamples                 |     SHORT |        1 |           | 1
invalid type value detected in Image::printIFDStructure:  250
Exiv2 exception in print action for file /Users/rmills/Downloads/004-heap-buffer-over.dms:
invalid type value detected in Image::printIFDStructure
681 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $
```

ASAN:

```
Same as above.
```

Files

004-heap-buffer-over	344 KB	23 Sep 2017	Zhu Liu