Exiv2 - Bug #1317

It is a heap-buffer-overflow in Exiv2::s2Data (types.cpp:383)

23 Sep 2017 04:09 - 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=1494781

./exiv2 006-heap-buffer-over
Error: Offset of directory Image, entry 0x00fe is out of bounds: Offset = 0x00000000; truncating the entry
Error: Offset of directory Image, entry 0x011b is out of bounds: Offset = 0x0080004a; truncating the entry
Error: Offset of directory Image, entry 0x02bc is out of bounds: Offset = 0x30000184; truncating the entry
Error: Upper boundary of data for directory Image, entry 0x83bb is out of bounds: Offset = 0x00003d7c, size = 26476552, exceeds buffer size by 26182327 Bytes; truncating the entry
Error: Directory Photo with 12336 entries considered invalid; not read.
==========
47847ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62100001661c at pc 0x7f3014bec6ff bp 0x7ffdc80d2f60 sp 0x7ffdc80d2f50
WRITE of size 1 at 0x62100001661c thread T0
#0 0x7f3014bec6fe in Exiv2::s2Data(unsigned char*, short, Exiv2::ByteOrder) /root/fuzzing/exiv2-trunk/src/types.cpp:383
#1 0x7f3014ac2831 in long Exiv2::toData<short>(unsigned char*, short, Exiv2::ByteOrder) /root/fuzzing/exiv2-trunk/include/exiv2/value.hpp:1477
#2 0x7f3014acbeeb in Exiv2::ValueType<short>::copy(unsigned char*, Exiv2::ByteOrder) const /root/fuzzing/exiv2-trunk/include/exiv2/value.hpp:1612
#3 0x7f3014abcaa4 in Exiv2::Exifdatum::copy(unsigned char*, Exiv2::ByteOrder) const /root/fuzzing/exiv2-trunk/src/exif.cpp:362
#4 0x7f3014bc1eff 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 0x7f3013e3b82f 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 0x7f30152686b2 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x996b2)
#1 0x7f3014bea695 in Exiv2::DataBuf::alloc(long) /root/fuzzing/exiv2-trunk/src/types.cpp:158
#2 0x7f3014bc1e62 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 0x7f3013e3b82f 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:383 Exiv2::s2Data(unsigned char*, 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
47847ABORTING
```

History

#1 - 25 Sep 2017 19:05 - Robin Mills

- Assignee deleted (Robin Mills)

- Priority changed from Urgent to Normal

#2 - 18 Sep 2018 12:47 - 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:

```
712 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 ~/Downloads/006-heap-buffer-over.dms
Error: Offset of directory Image, entry 0x00fe is out of bounds: Offset = 0x00000000; truncating the entry
Error: Offset of directory Image, entry 0x011b is out of bounds: Offset = 0x0080004a; truncating the entry
Error: Offset of directory Image, entry 0x02bc is out of bounds: Offset = 0x30000184; truncating the entry
Error: Upper boundary of data for directory Image, entry 0x83bb is out of bounds: Offset = 0x00003d7c, size =
26476552, exceeds buffer size by 26182327 Bytes; truncating the entry
Error: Directory Photo with 12336 entries considered invalid; not read.
File name       : /Users/rmills/Downloads/006-heap-buffer-over.dms
File size       : 309965 Bytes
MIME type       : image/tiff
Image size      : 17 x 12305
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 12305
White balance   :
Thumbnail       : None
Copyright       :
```

```
Exif comment    :

713 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 -pR ~/Downloads/006-heap-buffer-over.dms
STRUCTURE OF TIFF FILE (MM): /Users/rmills/Downloads/006-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 |           | 12305
      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 |           | 546
     142 | 0x011a XResolution                  |  RATIONAL |        1 |       304 | 355467264/1942487040
     154 | 0x011b YResolution                  |  RATIONAL |        1 |   8388682 | 8388682/0
     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 | 0008006013010053040
     214 | 0x013d Predictor                    |     SHORT |        1 |           | 48
     226 | 0x0152 ExtraSamples                 |     SHORT |        1 |           | 1
     238 | 0x02bc XMLPacket                    |      BYTE |    15152 | 805306756 | 0.......................
..... ...
Exiv2 exception in print action for file /Users/rmills/Downloads/006-heap-buffer-over.dms:
invalid memory allocation request
714 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $
```

ASAN build:

```
As above.
```

Files

006-heap-buffer-over	303 KB	23 Sep 2017	Zhu Liu