# Exiv2 - Bug #1319
## It is a heap-buffer-overflow in Exiv2::us2Data (types.cpp:346)

23 Sep 2017 04:15 - Zhu Liu

| | | | |
|---|---|---|---|
| **Status:** | New | **Start date:** | 23 Sep 2017 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | exif | **Estimated time:** | 0.00 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
  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*

### Files

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