Exiv2 - Bug #1321

Invalid memory address dereference in Exiv2::getULong(types.cpp:246)

23 Sep 2017 04:26 - Zhu Liu

Status:	Closed	**Start date:**	23 Sep 2017
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	metadata	**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=1494467

It's different from http://dev.exiv2.org/issues/1247 . it just can cause a invalid memory address dereference and crash.

./exiv2 02-Invalid-mem-def
ASAN:SIGSEGV ===
27020ERROR: AddressSanitizer: SEGV on unknown address 0x62a100000405 (pc 0x7f827e6cc4af bp 0x7ffdbe4d55b0 sp 0x7ffdbe4d55a0 T0)
#0 0x7f827e6cc4ae in Exiv2::getULong(unsigned char const*, Exiv2::ByteOrder) /root/fuzzing/exiv2-trunk/src/types.cpp:246
#1 0x7f827e6cc6cb in Exiv2::getURational(unsigned char const*, Exiv2::ByteOrder) /root/fuzzing/exiv2-trunk/src/types.cpp:257
#2 0x7f827e57323c in std::pair<unsigned int, unsigned int> Exiv2::getValue<std::pair<unsigned int, unsigned int> >(unsigned char const*, Exiv2::ByteOrder) (/usr/local/exiv2_ASAN/lib/libexiv2.so.26+0x31523c)
#3 0x7f827e580b4e in Exiv2::ValueType<std::pair<unsigned int, unsigned int> >::read(unsigned char const*, long, Exiv2::ByteOrder) /root/fuzzing/exiv2-trunk/include/exiv2/value.hpp:1586
#4 0x7f827e6c2d08 in Exiv2::Internal::TiffReader::readTiffEntry(Exiv2::Internal::TiffEntryBase*) /root/fuzzing/exiv2-trunk/src/tiffvisitor.cpp:1541
#5 0x7f827e6bf4be in Exiv2::Internal::TiffReader::visitEntry(Exiv2::Internal::TiffEntry*) /root/fuzzing/exiv2-trunk/src/tiffvisitor.cpp:1204
#6 0x7f827e68d97c in Exiv2::Internal::TiffEntry::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:896
#7 0x7f827e68d909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#8 0x7f827e68dcc2 in Exiv2::Internal::TiffDirectory::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:919
#9 0x7f827e68d909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#10 0x7f827e68e351 in Exiv2::Internal::TiffIfdMakernote::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:949
#11 0x7f827e68d909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#12 0x7f827e68e1bf in Exiv2::Internal::TiffMnEntry::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:938
#13 0x7f827e68d909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#14 0x7f827e68dcc2 in Exiv2::Internal::TiffDirectory::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:919
#15 0x7f827e68d909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#16 0x7f827e68e07e in Exiv2::Internal::TiffSubIfd::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:931
#17 0x7f827e68d909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#18 0x7f827e68dcc2 in Exiv2::Internal::TiffDirectory::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:919
#19 0x7f827e68d909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#20 0x7f827e6a6451 in Exiv2::Internal::TiffParserWorker::parse(unsigned char const*, unsigned int, unsigned int, Exiv2::Internal::TiffHeaderBase*) /root/fuzzing/exiv2-trunk/src/tiffimage.cpp:2011
#21 0x7f827e6a5267 in Exiv2::Internal::TiffParserWorker::decode(Exiv2::ExifData&, Exiv2::IptcData&, Exiv2::XmpData&, unsigned char const*, unsigned int, unsigned int, void (Exiv2::Internal::TiffDecoder::*)**(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&, unsigned int, Exiv2::Internal::IfdId))(Exiv2::Internal::TiffEntryBase const**), Exiv2::Internal::TiffHeaderBase*) /root/fuzzing/exiv2-trunk/src/tiffimage.cpp:1900
#22 0x7f827e6a3a82 in Exiv2::TiffParser::decode(Exiv2::ExifData&, Exiv2::IptcData&, Exiv2::XmpData&, unsigned char const*,

unsigned int) /root/fuzzing/exiv2-trunk/src/tiffimage.cpp:266
#23 0x7f827e5a043e in Exiv2::ExifParser::decode(Exiv2::ExifData&, unsigned char const*, unsigned int) /root/fuzzing/exiv2-trunk/src/exif.cpp:629
#24 0x7f827e5e0030 in Exiv2::JpegBase::readMetadata() /root/fuzzing/exiv2-trunk/src/jpgimage.cpp:386
#25 0x43ab02 in Action::Print::printSummary() /root/fuzzing/exiv2-trunk/src/actions.cpp:289
#26 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
#27 0x422129 in main /root/fuzzing/exiv2-trunk/src/exiv2.cpp:170
#28 0x7f827d91c82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#29 0x421af8 in _start (/usr/local/exiv2_ASAN/bin/exiv2+0x421af8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /root/fuzzing/exiv2-trunk/src/types.cpp:246 Exiv2::getULong(unsigned char const*, Exiv2::ByteOrder)
27020ABORTING

History

#1 - 25 Sep 2017 18:54 - Robin Mills

- Assignee deleted (Robin Mills)

- Priority changed from Urgent to Normal

#2 - 18 Sep 2018 12:40 - Robin Mills

- Category changed from exif to metadata

- 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:

```
708 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 ~/Downloads/02-Invalid-mem-def.dms
Exiv2 exception in print action for file /Users/rmills/Downloads/02-Invalid-mem-def.dms:
corrupted image metadata
709 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 -pa ~/Downloads/02-Invalid-mem-def.dms
Exiv2 exception in print action for file /Users/rmills/Downloads/02-Invalid-mem-def.dms:
corrupted image metadata
710 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 -pR ~/Downloads/02-Invalid-mem-def.dms
STRUCTURE OF JPEG FILE: /Users/rmills/Downloads/02-Invalid-mem-def.dms
 address | marker       |  length | data
       0 | 0xffd8 SOI
       2 | 0xff30
      20 | 0xffe1 APP1  |   21019 | Exif..II*.............00.....
  STRUCTURE OF TIFF FILE (II): MemIo
   address |    tag                              |      type |    count |    offset | value
        10 | 0x010e ImageDescription             |     ASCII |       11 |     12336 | 00000000000
        22 | 0x010f Make                         |     ASCII |        6 |       158 | NIKON
        34 | 0x0110 Model                        |     ASCII |        6 |       164 | 00000
        46 | 0x0112 Orientation                  |     SHORT |        1 |           | 12336
        58 | 0x011a XResolution                  |  RATIONAL |        1 |     12336 | 808464432/808464432
        70 | 0x011b YResolution                  |  RATIONAL |        1 |     12336 | 808464432/808464432
        82 | 0x0128 ResolutionUnit               |     SHORT |        1 |           | 12336
        94 | 0x0131 Software                     |     ASCII |    12336 |        48 | ......0000........00....
......00 ...
       106 | 0x0132 DateTime                     |     ASCII |    12336 |        48 | ......0000........00....
......00 ...
       118 | 0x0213 YCbCrPositioning             |     SHORT |        1 |           | 12336
       130 | 0x8769 ExifTag                      |      LONG |        1 |           | 236
    STRUCTURE OF TIFF FILE (II): MemIo
     address |    tag                              |      type |    count |    offset | value
         238 | 0x829a ExposureTime                 |  RATIONAL |        1 |       304 | 34209792/2416181248
         250 | 0x829d FNumber                      |  RATIONAL |        1 |     12336 | 808464432/808464432
         262 | 0x8822 ExposureProgram              |     SHORT |        1 |           | 2
         274 | 0x8827 ISOSpeedRatings              |     SHORT |        1 |           | 12336
         286 | 0x9000 ExifVersion                  | UNDEFINED |        4 |           | 0000
         298 | 0x9003 DateTimeOriginal             |     ASCII |    12336 |       522 | 00000000000000000000
```

```
0000000000 ...
         310 | 0x9004 DateTimeDigitized            |     ASCII |    12336 |       560 | 00....0000000000000000
0000..... ...
         322 | 0x9101 ComponentsConfiguration      | UNDEFINED |        4 |           | 0000
         334 | 0x9204 ExposureBiasValue            | SRATIONAL |        1 |       562 | 0/808464432
         346 | 0x9205 MaxApertureValue             |  RATIONAL |        1 |     12336 | 808464432/808464432
         358 | 0x9207 MeteringMode                 |     SHORT |        1 |           | 3
         370 | 0x9208 LightSource                  |     SHORT |        1 |           | 12336
         382 | 0x9209 Flash                        |     SHORT |        1 |           | 16
         394 | 0x920a FocalLength                  |  RATIONAL |        1 |     12336 | 808464432/808464432
         406 | 0x927c MakerNote                    | UNDEFINED |    12336 |       712 | Nikon.0000II*.........
......0000 ...
      STRUCTURE OF TIFF FILE (II): MemIo
       address |    tag                              |      type |    count |    offset | value
            10 | 0x0001 Version                      | UNDEFINED |        4 |           | 0000
            22 | 0x0002 ISOSpeed                     |     SHORT |        2 |           | 12336 12336
            34 | 0x0003 ColorMode                    |     ASCII |        6 |     12336 | 00...
            46 | 0x0004 Quality                      |     ASCII |        8 |       368 | 00000=0
            58 | 0x0005 WhiteBalance                 |     ASCII |       13 |       376 | 000000000000
            70 | 0x0006 Sharpening                   |     ASCII |        7 |     12336 | 00....
            82 | 0x0007 Focus                        |     ASCII |        7 |     12336 | 00....
            94 | 0x000a 0x000a                       |  RATIONAL |        1 |     12336 | 12336/0
           106 | 0x000f ISOSelection                 |     ASCII |        7 |     12336 | 00....
           118 | 0x0011 GPSImgDirection              |      LONG |        1 |           | 568
           130 | 0x0080 ImageAdjustment              |     ASCII |       14 |     12336 | 00..........
           142 | 0x0082 AuxiliaryLens                |     ASCII |       13 |     12336 | 00.........
           154 | 0x0086 DigitalZoom                  |  RATIONAL |        1 |4294967088 | 4294967088/0
           166 | 0x0080 ImageAdjustment              | UNDEFINED |        4 |           | 0000
Exiv2 exception in print action for file /Users/rmills/Downloads/02-Invalid-mem-def.dms:
invalid memory allocation request
711 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $
```

ASAN build:

```
As above.
```

#3 - 02 Oct 2018 09:28 - Robin Mills

- Subject changed from Invalid memory address dereference in Exiv2::getULong(types.cpp:246) to Invalid memory address dereference in Exiv2::getULong(types.cpp:246)

Files

02-Invalid-mem-def	29.4 KB	23 Sep 2017	Zhu Liu