Exiv2 - Bug #1318

Invalid memory address dereference in Exiv2::StringValueBase::read (in value.cpp:302)

23 Sep 2017 04:14 - 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=1494780

./exiv2 005-invalid-mem
Warning: Directory Image, entry 0x011a has unknown Exif (TIFF) type 64772; setting type size 1.
Error: Upper boundary of data for directory Image, entry 0x011b is out of bounds: Offset = 0x00000030, size = 1073741832, exceeds buffer size by 1073734073 Bytes; truncating the entry
Error: Upper boundary of data for directory Photo, entry 0x9003 is out of bounds: Offset = 0x000001f8, size = 3538992, exceeds buffer size by 3531689 Bytes; truncating the entry
Warning: Directory Nikon3 has an unexpected next pointer; ignored.
ASAN:SIGSEGV ===
11802ERROR: AddressSanitizer: SEGV on unknown address 0x62410000c2c3 (pc 0x7f69ca832cf0 bp 0x7ffc8db8ae20 sp 0x7ffc8db8a5a8 T0)
#0 0x7f69ca832cef (/lib/x86_64-linux-gnu/libc.so.6+0x160cef)
#1 0x7f69cbb125d0 in *_asan_memcpy (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x8c5d0)*
*#2 0x7f69cadd3b06 in void std::*_cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >::_M_construct<char const*>(char const*, char const*, std::forward_iterator_tag) (/usr/lib/x86_64-linux-gnu/libstdc++.so.6+0x121b06)
#3 0x7f69cadd3c04 in std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >::basic_string(char const*, unsigned long, std::allocator<char> const&) (/usr/lib/x86_64-linux-gnu/libstdc++.so.6+0x121c04)
#4 0x7f69cb4a9057 in Exiv2::StringValueBase::read(unsigned char const*, long, Exiv2::ByteOrder) /root/fuzzing/exiv2-trunk/src/value.cpp:302
#5 0x7f69cb498d08 in Exiv2::Internal::TiffReader::readTiffEntry(Exiv2::Internal::TiffEntryBase*) /root/fuzzing/exiv2-trunk/src/tiffvisitor.cpp:1541
#6 0x7f69cb4954be in Exiv2::Internal::TiffReader::visitEntry(Exiv2::Internal::TiffEntry*) /root/fuzzing/exiv2-trunk/src/tiffvisitor.cpp:1204
#7 0x7f69cb46397c in Exiv2::Internal::TiffEntry::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:896
#8 0x7f69cb463909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#9 0x7f69cb463cc2 in Exiv2::Internal::TiffDirectory::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:919
#10 0x7f69cb463909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#11 0x7f69cb464351 in Exiv2::Internal::TiffIfdMakernote::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:949
#12 0x7f69cb463909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#13 0x7f69cb4641bf in Exiv2::Internal::TiffMnEntry::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:938
#14 0x7f69cb463909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#15 0x7f69cb463cc2 in Exiv2::Internal::TiffDirectory::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:919
#16 0x7f69cb463909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#17 0x7f69cb46407e in Exiv2::Internal::TiffSubIfd::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:931
#18 0x7f69cb463909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#19 0x7f69cb463cc2 in Exiv2::Internal::TiffDirectory::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:919
#20 0x7f69cb463909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#21 0x7f69cb47c451 in Exiv2::Internal::TiffParserWorker::parse(unsigned char const*, unsigned int, unsigned int,

```
Exiv2::Internal::TiffHeaderBase*) /root/fuzzing/exiv2-trunk/src/tiffimage.cpp:2011
#22 0x7f69cb47b267 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
#23 0x7f69cb479a82 in Exiv2::TiffParser::decode(Exiv2::ExifData&, Exiv2::IptcData&, Exiv2::XmpData&, unsigned char const*, unsigned int) /root/fuzzing/exiv2-trunk/src/tiffimage.cpp:266
#24 0x7f69cb37643e in Exiv2::ExifParser::decode(Exiv2::ExifData&, unsigned char const*, unsigned int) /root/fuzzing/exiv2-trunk/src/exif.cpp:629
#25 0x7f69cb3b6030 in Exiv2::JpegBase::readMetadata() /root/fuzzing/exiv2-trunk/src/jpgimage.cpp:386
#26 0x43ab02 in Action::Print::printSummary() /root/fuzzing/exiv2-trunk/src/actions.cpp:289
#27 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
#28 0x422129 in main /root/fuzzing/exiv2-trunk/src/exiv2.cpp:170
#29 0x7f69ca6f282f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#30 0x421af8 in _start (/usr/local/exiv2_ASAN/bin/exiv2+0x421af8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ??:0 ??
11802ABORTING
```

History

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

- Assignee deleted (Robin Mills)

- Priority changed from Urgent to Normal

#2 - 18 Sep 2018 12:49 - 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:

```
719 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 ~/Downloads/005-invalid-mem.dms
Warning: Directory Image, entry 0x011a has unknown Exif (TIFF) type 64772; setting type size 1.
Error: Upper boundary of data for directory Image, entry 0x011b is out of bounds: Offset = 0x00000030, size = 1073741832, exceeds buffer size by 1073734073 Bytes; truncating the entry
Error: Upper boundary of data for directory Photo, entry 0x9003 is out of bounds: Offset = 0x000001f8, size = 3538992, exceeds buffer size by 3531689 Bytes; truncating the entry
Warning: Directory Nikon3 has an unexpected next pointer; ignored.
Exiv2 exception in print action for file /Users/rmills/Downloads/005-invalid-mem.dms:
corrupted image metadata
720 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 -pR ~/Downloads/005-invalid-mem.dms
STRUCTURE OF JPEG FILE: /Users/rmills/Downloads/005-invalid-mem.dms
 address | marker       |  length | data
       0 | 0xffd8 SOI
       2 | 0xff30
      20 | 0xffe1 APP1  |    7815 | Exif..II*...............0......
  STRUCTURE OF TIFF FILE (II): MemIo
   address |    tag                              |      type |    count |    offset | value
        10 | 0x010e ImageDescription             |     ASCII |       11 |        48 | ......0000.
        22 | 0x010f Make                         |     ASCII |        6 |       158 | NIKON
        34 | 0x0110 Model                        |     ASCII |        6 |       164 | 00000
        46 | 0x0112 Orientation                  |     SHORT |        1 |           | 12336
invalid type value detected in Image::printIFDStructure:  64772
Exiv2 exception in print action for file /Users/rmills/Downloads/005-invalid-mem.dms:
invalid type value detected in Image::printIFDStructure
721 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::StringValueBase::read (in value.cpp:302) to Invalid memory address dereference in Exiv2::StringValueBase::read (in value.cpp:302)

Files

005-invalid-mem	19.6 KB	23 Sep 2017	Zhu Liu