Exiv2 - Bug #1315

Invalid memory address dereference in Exiv2::DataValue::read (value.cpp:193)

23 Sep 2017 03:59 - 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=1494786

./exiv2 008-invalid-mem
Warning: Directory Image, entry 0xff13 has unknown Exif (TIFF) type 65535; setting type size 1.
Error: Offset of directory Image, entry 0xff13 is out of bounds: Offset = 0x30303030; truncating the entry
Warning: Directory Photo has an unexpected next pointer; ignored.
Error: Offset of directory Photo, entry 0x8827 is out of bounds: Offset = 0x30303030; truncating the entry
Error: Directory Photo, entry 0x9204 has invalid size 4286513153*8; skipping entry.
Warning: Directory Nikon3 has an unexpected next pointer; ignored.
Error: Upper boundary of data for directory Nikon3, entry 0x0004 is out of bounds: Offset = 0x00000170, size = 1376264, exceeds buffer size by 1369403 Bytes; truncating the entry
Error: Offset of directory Nikon3, entry 0x0006 is out of bounds: Offset = 0x0000e803; truncating the entry
Error: Directory NikonPreview with 12336 entries considered invalid; not read.
Warning: Directory Nikon3, entry 0x0095 has unknown Exif (TIFF) type 2562; setting type size 1.
Error: Offset of directory Nikon3, entry 0x009c is out of bounds: Offset = 0x000ffff8; truncating the entry
ASAN:SIGSEGV ===
33537ERROR: AddressSanitizer: SEGV on unknown address 0x62410000c272 (pc 0x7f40f6995960 bp 0x7ffcb5b71620 sp 0x7ffcb5b70da8 T0)
#0 0x7f40f699595f (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xaa95f)
#1 0x7f40f6977e8d in *_asan_memmove (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x8ce8d)*
#2 0x7f40f61b9ada in unsigned char std::*_copy_move<false, true, std::random_access_iterator_tag>::__copy_m<unsigned char>(unsigned char const*, unsigned char const*, unsigned char*) /usr/include/c++/5/bits/stl_algobase.h:384
#3 0x7f40f6289d9a in unsigned char* std::__copy_move_a<false, unsigned char const*, unsigned char*>(unsigned char const*, unsigned char const*, unsigned char*) /usr/include/c++/5/bits/stl_algobase.h:402
#4 0x7f40f6289291 in unsigned char* std::__copy_move_a2<false, unsigned char const*, unsigned char*>(unsigned char const*, unsigned char const*, unsigned char*) /usr/include/c++/5/bits/stl_algobase.h:440
#5 0x7f40f6288fa0 in unsigned char* std::copy<unsigned char const*, unsigned char*>(unsigned char const*, unsigned char const*, unsigned char*) /usr/include/c++/5/bits/stl_algobase.h:472
#6 0x7f40f631c763 in unsigned char* std::__uninitialized_copy<true>::__uninit_copy<unsigned char const*, unsigned char*>(unsigned char const*, unsigned char const*, unsigned char*) /usr/include/c++/5/bits/stl_uninitialized.h:93
#7 0x7f40f631bde5 in unsigned char* std::uninitialized_copy<unsigned char const*, unsigned char*>(unsigned char const*, unsigned char const*, unsigned char*) /usr/include/c++/5/bits/stl_uninitialized.h:126
#8 0x7f40f631b353 in unsigned char* std::__uninitialized_copy_a<unsigned char const*, unsigned char*, unsigned char>(unsigned char const*, unsigned char const*, unsigned char*, std::allocator<unsigned char>&) /usr/include/c++/5/bits/stl_uninitialized.h:281
#9 0x7f40f631b270 in unsigned char* std::vector<unsigned char, std::allocator<unsigned char> >::_M_allocate_and_copy<unsigned char const*>(unsigned long, unsigned char const*, unsigned char const*) /usr/include/c++/5/bits/stl_vector.h:1227
#10 0x7f40f6319f66 in void std::vector<unsigned char, std::allocator<unsigned char> >::_M_assign_aux<unsigned char const*>(unsigned char const*, unsigned char const*, std::forward_iterator_tag) /usr/include/c++/5/bits/vector.tcc:273
#11 0x7f40f63190d5 in void std::vector<unsigned char, std::allocator<unsigned char> >::_M_assign_dispatch<unsigned char const*>(unsigned char const*, unsigned char const*, std::__false_type) /usr/include/c++/5/bits/stl_vector.h:1336
#12 0x7f40f6317cf1 in void std::vector<unsigned char, std::allocator<unsigned char> >::assign<unsigned char const*>(unsigned char const*, unsigned char const*) /usr/include/c++/5/bits/stl_vector.h:516
#13 0x7f40f630d2ec in Exiv2::DataValue::read(unsigned char const*, long, Exiv2::ByteOrder) /root/fuzzing/exiv2-trunk/src/value.cpp:193
#14 0x7f40f62fdd08 in Exiv2::Internal::TiffReader::readTiffEntry(Exiv2::Internal::TiffEntryBase*) /root/fuzzing/exiv2-trunk/src/tiffvisitor.cpp:1541
#15 0x7f40f62fa4be in Exiv2::Internal::TiffReader::visitEntry(Exiv2::Internal::TiffEntry*) /root/fuzzing/exiv2-trunk/src/tiffvisitor.cpp:1204
#16 0x7f40f62c897c in Exiv2::Internal::TiffEntry::doAccept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:896
#17 0x7f40f62c8909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&) /root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#18 0x7f40f62c8cc2 in Exiv2::Internal::TiffDirectory::doAccept(Exiv2::Internal::TiffVisitor&)

/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:919
#19 0x7f40f62c8909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#20 0x7f40f62c9351 in Exiv2::Internal::TiffIfdMakernote::doAccept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:949
#21 0x7f40f62c8909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#22 0x7f40f62c91bf in Exiv2::Internal::TiffMnEntry::doAccept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:938
#23 0x7f40f62c8909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#24 0x7f40f62c8cc2 in Exiv2::Internal::TiffDirectory::doAccept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:919
#25 0x7f40f62c8909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#26 0x7f40f62c907e in Exiv2::Internal::TiffSubIfd::doAccept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:931
#27 0x7f40f62c8909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#28 0x7f40f62c8cc2 in Exiv2::Internal::TiffDirectory::doAccept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:919
#29 0x7f40f62c8909 in Exiv2::Internal::TiffComponent::accept(Exiv2::Internal::TiffVisitor&)
/root/fuzzing/exiv2-trunk/src/tiffcomposite.cpp:891
#30 0x7f40f62e1451 in Exiv2::Internal::TiffParserWorker::parse(unsigned char const*, unsigned int, unsigned int,
Exiv2::Internal::TiffHeaderBase*) /root/fuzzing/exiv2-trunk/src/tiffimage.cpp:2011
#31 0x7f40f62e0267 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
#32 0x7f40f62dea82 in Exiv2::TiffParser::decode(Exiv2::ExifData&, Exiv2::IptcData&, Exiv2::XmpData&, unsigned char const*,
unsigned int) /root/fuzzing/exiv2-trunk/src/tiffimage.cpp:266
#33 0x7f40f61db43e in Exiv2::ExifParser::decode(Exiv2::ExifData&, unsigned char const*, unsigned int)
/root/fuzzing/exiv2-trunk/src/exif.cpp:629
#34 0x7f40f621b030 in Exiv2::JpegBase::readMetadata() /root/fuzzing/exiv2-trunk/src/jpgimage.cpp:386
#35 0x43ab02 in Action::Print::printSummary() /root/fuzzing/exiv2-trunk/src/actions.cpp:289
#36 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
#37 0x422129 in main /root/fuzzing/exiv2-trunk/src/exiv2.cpp:170
#38 0x7f40f555782f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#39 0x421af8 in _start (/usr/local/exiv2_ASAN/bin/exiv2+0x421af8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ??:0 ??
33537ABORTING

History

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

- Assignee deleted (Robin Mills)

- Priority changed from Urgent to Normal

#2 - 18 Sep 2018 13:14 - 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:

```
829 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 ~/Downloads/008-invalid-mem.dms
Warning: Directory Image, entry 0xff13 has unknown Exif (TIFF) type 65535; setting type size 1.
Error: Offset of directory Image, entry 0xff13 is out of bounds: Offset = 0x30303030; truncating the entry
Warning: Directory Photo has an unexpected next pointer; ignored.
```

```
Error: Offset of directory Photo, entry 0x8827 is out of bounds: Offset = 0x30303030; truncating the entry
Error: Directory Photo, entry 0x9204 has invalid size 4286513153*8; skipping entry.
Warning: Directory Nikon3 has an unexpected next pointer; ignored.
Error: Upper boundary of data for directory Nikon3, entry 0x0004 is out of bounds: Offset = 0x00000170, size =
 1376264, exceeds buffer size by 1369403 Bytes; truncating the entry
Error: Offset of directory Nikon3, entry 0x0006 is out of bounds: Offset = 0x0000e803; truncating the entry
Error: Directory NikonPreview with 12336 entries considered invalid; not read.
Warning: Directory Nikon3, entry 0x0095 has unknown Exif (TIFF) type 2562; setting type size 1.
Error: Offset of directory Nikon3, entry 0x009c is out of bounds: Offset = 0x000ffff8; truncating the entry
Exiv2 exception in print action for file /Users/rmills/Downloads/008-invalid-mem.dms:
corrupted image metadata
830 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 -pR ~/Downloads/008-invalid-mem.dms
STRUCTURE OF JPEG FILE: /Users/rmills/Downloads/008-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 | ......*000.
        22 | 0x010f Make                         |     ASCII |        6 |       158 | NIKON
        34 | 0x0110 Model                        |     ASCII |        6 |       164 | 00000
        46 | 0x0112 Orientation                  |     SHORT |        1 |           | 12330
        58 | 0x011a XResolution                  |  RATIONAL |        1 |        48 | 65539/808058880
        70 | 0x011b YResolution                  |  RATIONAL |        1 |        48 | 65539/808058880
        82 | 0x0128 ResolutionUnit               |     SHORT |        1 |           | 12336
        94 | 0x0131 Software                     |     ASCII |       48 |        48 | ......*000........0.....
......0 ...
       106 | 0x0132 DateTime                     |     ASCII |       48 |        48 | ......*000........0.....
......0 ...
invalid type value detected in Image::printIFDStructure:  65535
Exiv2 exception in print action for file /Users/rmills/Downloads/008-invalid-mem.dms:
invalid type value detected in Image::printIFDStructure
831 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $
```

ASAN build:

```
As above.
```

Files

008-invalid-mem	7.72 KB	23 Sep 2017	Zhu Liu