Example output:

ASAN:SIGSEGV

===

==11348==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f440c6fa8c8 sp 0x7ffd88d08360 bp 0x7ffd88d08950 T0)

==11348==WARNING: Trying to symbolize code, but external symbolizer is not initialized!

#0 0x7f440c6fa8c7 (/home/lolopop/projects/exiv2/build-clang/exiv2/src/libexiv2.so.26+0x9328c7)

#1 0x7f440c6ead13 (/home/lolopop/projects/exiv2/build-clang/exiv2/src/libexiv2.so.26+0x922d13)

#2 0x7f440c6f9303 (/home/lolopop/projects/exiv2/build-clang/exiv2/src/libexiv2.so.26+0x931303)

#3 0x7f440c6ead13 (/home/lolopop/projects/exiv2/build-clang/exiv2/src/libexiv2.so.26+0x922d13)

#4 0x7f440c6e8507 (/home/lolopop/projects/exiv2/build-clang/exiv2/src/libexiv2.so.26+0x920507)

#5 0x7f440c6e45fa (/home/lolopop/projects/exiv2/build-clang/exiv2/src/libexiv2.so.26+0x91c5fa)

#6 0x7f440c766014 (/home/lolopop/projects/exiv2/build-clang/exiv2/src/libexiv2.so.26+0x99e014)

#7 0x7f440c7622d8 (/home/lolopop/projects/exiv2/build-clang/exiv2/src/libexiv2.so.26+0x99a2d8)

#8 0x7f440c761278 (/home/lolopop/projects/exiv2/build-clang/exiv2/src/libexiv2.so.26+0x999278)

#9 0x47d99d (/home/lolopop/projects/exiv2/build-clang/exiv2/bin/convert-test+0x47d99d)

#10 0x7f440a9adf44 (/lib/x86_64-linux-gnu/libc.so.6+0x21f44)

#11 0x47cc0c (/home/lolopop/projects/exiv2/build-clang/exiv2/bin/convert-test+0x47cc0c)

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV ??:0 ??

==11348==ABORTING

Debug info:

invalid type value detected in Image::printIFDStructure: 256

Error: Directory Image: Next pointer is out of bounds; ignored.

Warning: Directory Image, entry 0x0111 has unknown Exif (TIFF) type 256; setting type size 1.

Error: Directory Image, entry 0x0111 has invalid size 1342177280*1; skipping entry.

Warning: Directory Image, entry 0x0111: Size or data offset value not set, ignoring them.

Warning: Directory Image, entry 0x0501 has unknown Exif (TIFF) type 256; setting type size 1.

Error: Directory Image, entry 0x0501 has invalid size 1476395008*1; skipping entry.

Warning: Directory Image, entry 0x0301 has unknown Exif (TIFF) type 256; setting type size 1.

Error: Offset of directory Image, entry 0x0301 is out of bounds: Offset = 0x28000000; truncating the entry

Warning: Directory Image, entry 0x0301 has unknown Exif (TIFF) type 256; setting type size 1.

Error: Offset of directory Image, entry 0x0301 is out of bounds: Offset = 0x29000000; truncating the entry

Warning: Directory Image, entry 0x0301 has unknown Exif (TIFF) type 512; setting type size 1.

Error: Directory Image: Next pointer is out of bounds; ignored.

Warning: Directory Image, entry 0x0111 has unknown Exif (TIFF) type 256; setting type size 1.

Error: Directory Image, entry 0x0111 has invalid size 1342177280*1; skipping entry.

Warning: Directory Image, entry 0x0111: Size or data offset value not set, ignoring them.

Warning: Directory Image, entry 0x0501 has unknown Exif (TIFF) type 256; setting type size 1.

Error: Directory Image, entry 0x0501 has invalid size 1476395008*1; skipping entry.

Warning: Directory Image, entry 0x0301 has unknown Exif (TIFF) type 256; setting type size 1.

Error: Offset of directory Image, entry 0x0301 is out of bounds: Offset = 0x28000000; truncating the entry

Warning: Directory Image, entry 0x0301 has unknown Exif (TIFF) type 256; setting type size 1.

Error: Offset of directory Image, entry 0x0301 is out of bounds: Offset = 0x29000000; truncating the entry

Warning: Directory Image, entry 0x0301 has unknown Exif (TIFF) type 512; setting type size 1.

Program received signal SIGSEGV, Segmentation fault.

0x00007ffff7a25c46 in Exiv2::Internal::TiffImageEntry::doWriteImage (this=0x6188b0, ioWrapper=...) at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:1614

1614 uint32_t len = pValue()->sizeDataArea();

(gdb) p pValue()

$3 = (const Exiv2::Value *) 0x0

(gdb) bt

#0 0x00007ffff7a25c46 in Exiv2::Internal::TiffImageEntry::doWriteImage (this=0x6188b0, ioWrapper=...) at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:1614

#1 0x00007ffff7a259dd in Exiv2::Internal::TiffComponent::writeImage (this=0x6188b0, ioWrapper=..., byteOrder=Exiv2::littleEndian) at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:1559

#2 0x00007ffff7a25a99 in Exiv2::Internal::TiffDirectory::doWriteImage (this=0x619d10, ioWrapper=..., byteOrder=Exiv2::littleEndian)

at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:1574

#3 0x00007ffff7a259dd in Exiv2::Internal::TiffComponent::writeImage (this=0x619d10, ioWrapper=..., byteOrder=Exiv2::littleEndian) at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:1559

#4 0x00007ffff7a2436b in Exiv2::Internal::TiffDirectory::doWrite (this=0x619d10, ioWrapper=..., byteOrder=Exiv2::littleEndian, offset=8, valueIdx=4294967295, dataIdx=4294967295,

imageIdx=@0x7fffffffde98: 3240) at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:1204

#5 0x00007ffff7a23c2f in Exiv2::Internal::TiffComponent::write (this=0x619d10, ioWrapper=..., byteOrder=Exiv2::littleEndian, offset=8, valueIdx=4294967295, dataIdx=4294967295,

imageIdx=@0x7fffffffde98: 3240) at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:1079

#6 0x00007ffff7a2f915 in Exiv2::Internal::TiffParserWorker::encode (io=..., pData=0x7ffff7ff4000 "II*", size=459, exifData=..., iptcData=..., xmpData=..., root=131072,

findEncoderFct=0x7ffff7a2ef9a <Exiv2::Internal::TiffMapping::findEncoder(std::string const&, unsigned int, Exiv2::Internal::IfdId)>, pHeader=0x6124b0, pOffsetWriter=0x0)

at /home/lolopop/projects/exiv2/src/tiffimage.cpp:1980

#7 0x00007ffff7a2e987 in Exiv2::TiffParser::encode (io=..., pData=0x7ffff7ff4000 "II*", size=459, byteOrder=Exiv2::littleEndian, exifData=..., iptcData=..., xmpData=...)

at /home/lolopop/projects/exiv2/src/tiffimage.cpp:306

#8 0x00007ffff7a2e75d in Exiv2::TiffImage::writeMetadata (this=0x6072b0) at /home/lolopop/projects/exiv2/src/tiffimage.cpp:249

#9 0x0000000000402c5d in main (argc=2, argv=0x7fffffffe508) at /home/lolopop/projects/exiv2/samples/convert-test.cpp:30

Explanation：

I see the tiff structure of the crash161 file by using 010edit.exe

struct IFD ifd[0]	18: ImageWidth
uint16 numentries	18
struct ENT dir[0]	ImageWidth (256): eSHORT
struct ENT dir[1]	StripOffsets (273): eSHORT
struct ENT dir[2]	BitsPerSample (258): eSHORT
struct ENT dir[3]	Compression (259): eSHORT
struct ENT dir[4]	PhotometricInterpretation (262): eSHORT
struct ENT dir[5]	FillOrder (266): eSHORT
struct ENT dir[6]	DocumentName (269): eASCII
struct ENT dir[7]	StripOffsets (273): eLONG
struct ENT dir[8]	Orientation (274): eSHORT
struct ENT dir[9]	SamplesPerPixel (277): eSHORT
struct ENT dir[10]	RowsPerStrip (278): eSHORT
struct ENT dir[11]	StripByteCounts (279): eLONG
struct ENT dir[12]	XResolution (282): eRATIONAL
struct ENT dir[13]	StripOffsets (273):
struct ENT dir[14]	(1281):
struct ENT dir[15]	(769):
struct ENT dir[16]	(769):
struct ENT dir[17]	(769):
uint32 offset	30000301h

struct ENT dir[14]	(1281):
enum TAG tag	1281
enum TAGTYPE typ	256
uint32 count	1476395008
uint32 valOffset	1C0D0001h
struct ENT dir[15]	(769):
enum TAG tag	769
enum TAGTYPE typ	256
uint32 count	16777216
uint32 valOffset	28000000h
struct ENT dir[16]	(769):
enum TAG tag	769
enum TAGTYPE typ	256
uint32 count	16777216
uint32 valOffset	29000000h
struct ENT dir[17]	(769):
enum TAG tag	769
enum TAGTYPE typ	512
uint32 count	0
uint32 valOffset	40000100h
uint32 offset	30000301h

The structure of the normal tiff file is as follows

struct IFD ifd	18: ImageWidth
uint16 numentries	18
struct ENT dir[0]	ImageWidth (256): eSHORT
struct ENT dir[1]	ImageLength (257): eSHORT
struct ENT dir[2]	BitsPerSample (258): eSHORT
struct ENT dir[3]	Compression (259): eSHORT
struct ENT dir[4]	PhotometricInterpretation (262): eSHORT
struct ENT dir[5]	FillOrder (266): eSHORT
struct ENT dir[6]	DocumentName (269): eASCII
struct ENT dir[7]	StripOffsets (273): eLONG
struct ENT dir[8]	Orientation (274): eSHORT
struct ENT dir[9]	SamplesPerPixel (277): eSHORT
struct ENT dir[10]	RowsPerStrip (278): eSHORT
struct ENT dir[11]	StripByteCounts (279): eLONG
struct ENT dir[12]	XResolution (282): eRATIONAL
struct ENT dir[13]	YResolution (283): eRATIONAL
struct ENT dir[14]	PlanarConfiguration (284): eSHORT
struct ENT dir[15]	ResolutionUnit (296): eSHORT
struct ENT dir[16]	PageNumber (297): eSHORT
struct ENT dir[17]	ColorMap (320): eSHORT
uint32 offset	0h

struct IFD ifd	
uint16 numentries	18
struct ENT dir[0]	ImageWidth (256): eSHORT
enum TAG tag	ImageWidth (256)
enum TAGTYPE typ	eSHORT (3)
uint32 count	1
uint16 value	32
uint16 padding	0
struct ENT dir[1]	ImageLength (257): eSHORT
enum TAG tag	ImageLength (257)
enum TAGTYPE typ	eSHORT (3)
uint32 count	1
uint16 value	32
uint16 padding	0
struct ENT dir[2]	BitsPerSample (258): eSHORT
enum TAG tag	BitsPerSample (258)
enum TAGTYPE typ	eSHORT (3)
uint32 count	1
uint16 value	4
uint16 padding	0

You can see structure exception of tiff file on crash161 file, the last four struct stored data is wrong.

By looking at the source code, the value of pValue () is affected by the value of pValue_.

```
const Value* pValue()   const { return pValue_; }
//@}
```

The value of pValue_ is assigned by these two methods.

```
TiffEntryBase::TiffEntryBase(uint16_t tag, IfdId group, TiffType tiffType)
    : TiffComponent(tag, group),
      tiffType_(tiffType), count_(0), offset_(0),
      size_(0), pData_(0), isMalloced_(false), idx_(0),
      pValue_(0)
{
}
```

```
TiffEntryBase::TiffEntryBase(const TiffEntryBase& rhs)
    : TiffComponent(rhs),
      tiffType_(rhs.tiffType_),
      count_(rhs.count_),
      offset_(rhs.offset_),
      size_(rhs.size_),
      pData_(rhs.pData_),
      isMalloced_(rhs.isMalloced_),
      idx_(rhs.idx_),
      pValue_(rhs.pValue_ ? rhs.pValue_->clone().release() : 0)
{
    if (rhs.isMalloced_) {
        pData_ = new byte[rhs.size_];
        memcpy(pData_, rhs.pData_, rhs.size_);
    }
}
```

Here we are denoted as TiffEntryBase1 and TiffEntryBase2, respectively.

Break down these two methods,

```
9       breakpoint     keep y   0x00007fa6236b3d01 in Exiv2::Internal::TiffEntryBase::TiffEntryBase(Exiv2::Internal::TiffEntryBase const&)
                                                   at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:260
10      hw watchpoint  keep y                      -location pValue_
11      breakpoint     keep y   0x00007fa6236b2f19 in Exiv2::Internal::TiffEntryBase::TiffEntryBase(unsigned short, Exiv2::Internal::IfdId, unsigned short)
                                                   at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:105
```

The program parses the data in the struct IFD ifd structure which contains 18 structures.

The program calls TiffEntryBase1 to get the tag in each structure. As shown below, it will cycle 18 times here.

```
Breakpoint 11, Exiv2::Internal::TiffEntryBase::TiffEntryBase (this=0x15c7660, tag=256, group=Exiv2::Internal::ifd0Id, tiffType=7) at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:105
105             pValue_(0)
```

The program calls TiffEntryBase2 to get the other parameters in each structure.

```
Breakpoint 9, Exiv2::Internal::TiffEntryBase::TiffEntryBase (this=0x15d0d90, rhs=...) at /home/lolopop/projects/exiv2/src/tiffcomposite.cpp:260
260             pValue_(rhs.pValue_ ? rhs.pValue_->clone().release() : 0)
(rr)
```

Since the last four of the 18 structures were wrong, TiffEntryBase2 only called 14 times. The 15th call is TiffEntryBase1, where pValue_ is equal to 0x0.

The program will call the following code

```
uint32_t TiffComponent::writeImage(IoWrapper& ioWrapper,
                                   ByteOrder byteOrder) const
{
    return doWriteImage(ioWrapper, byteOrder);
} // TiffComponent::writeImage
```

When you parse the wrong structure, the TiffImageEntry :: doWriteImage method is called.

```
1611:    uint32_t TiffImageEntry::doWriteImage(IoWrapper& ioWrapper,
1612:                                          ByteOrder  /*byteOrder*/) const
1613:    {
1614:        uint32_t len = pValue()->sizeDataArea();
1615:        if (len > 0) {
1616: #ifdef DEBUG
1617:            std::cerr << "TiffImageEntry, Directory " << groupName(group())
1618:                      << ", entry 0x" << std::setw(4)
1619:                      << std::setfill('0') << std::hex << tag() << std::dec
1620:                      << ": Writing data area, size = " << len;
1621: #endif
1622:            DataBuf buf = pValue()->dataArea();
1623:            ioWrapper.write(buf.pData_, buf.size_);
1624:            uint32_t align = len & 1;       // Align image data to word boundary
1625:            if (align) ioWrapper.putb(0x0);
1626:            len += align;
1627:        }
1628:        else {
1629: #ifdef DEBUG
1630:            std::cerr << "TiffImageEntry, Directory " << groupName(group())
1631:                      << ", entry 0x" << std::setw(4)
1632:                      << std::setfill('0') << std::hex << tag() << std::dec
1633:                      << ": Writing " << strips_.size() << " strips";
1634: #endif
1635:            len = 0;
1636:            for (Strips::const_iterator i = strips_.begin(); i != strips_.end(); ++i) {
1637:                ioWrapper.write(i->first, i->second);
1638:                len += i->second;
```

At this point, pValue_ = 0x0, so pValue () gets the value 0x0.

So a Segmentation fault occurs.

Author

Name: lolopop and Young_X
Org: IIE (http:// iie.ac.cn)