Exiv2 - Bug #1305

Segmentation fault on certain image

28 Jul 2017 11:17 - Anonymous

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
<th>Start date:</th>
<th>28 Jul 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>Robin Mills</td>
<td>% Done:</td>
<td>100%</td>
</tr>
<tr>
<td>Category:</td>
<td>miscellaneous</td>
<td>Estimated time:</td>
<td>8.00 hours</td>
</tr>
<tr>
<td>Target version:</td>
<td>0.27</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description**

Originally discovered in Gwenview which uses libexiv2 [https://bugs.kde.org/show_bug.cgi?id=382842](https://bugs.kde.org/show_bug.cgi?id=382842)
The problematic image attached.

libexiv2 0.26 openSUSE Tumbleweed 64 bit

Thread 1 "gwenview" received signal SIGSEGV, Segmentation fault.
0x00007fff180f5f in Exiv2::ExifData::findKey(Exiv2::ExifKey const&) const () from /usr/lib64/libexiv2.so.26 (gdb) bt
#0 0x00007fff180f5f in Exiv2::ExifData::findKey(Exiv2::ExifKey const&) const () from /usr/lib64/libexiv2.so.26
#1 0x00007fff18556a1 in Exiv2::Internal::PentaxMakerNote::printShutterCount(std::ostream&, Exiv2::Value const&, Exiv2::ExifData const*) () from /usr/lib64/libexiv2.so.26
#2 0x00007fff7460c0f in ?? () from /usr/lib64/libgwenviewlib.so.5
#3 0x00007fff746bb89 in Gwenview::ImageMetaInfoModel::setExiv2Image(Exiv2::Image const*) () from /usr/lib64/libgwenviewlib.so.5
#4 0x00007fff74207b7 in Gwenview::ImageMetaInfoModel::setExiv2Image(Exiv2::Image const*) () from /usr/lib64/libgwenviewlib.so.5
#5 0x00007fff741f7d1 in ?? () from /usr/lib64/libgwenviewlib.so.5
#6 0x00007fff742af11 in ?? () from /usr/lib64/libgwenviewlib.so.5
#7 0x00007fff743a7645a in QMetaObject::activate(QObject*, int, int, void**) () from /usr/lib64/libQt5Core.so.5
#8 0x00007fff8373103 in QFutureWatcherBase::event(QEvent*) () from /usr/lib64/libQt5Core.so.5
#9 0x00007fff840a93c in QApplicationPrivate::notify_helper(QObject*, QEvent*) () from /usr/lib64/libQt5Widgets.so.5
#10 0x00007fff8411cb4 in QApplication::notify(QObject*, QEvent*) () from /usr/lib64/libQt5Widgets.so.5
#11 0x00007fff841f8f8 in QCOREApplication::notifyInternal2(QObject*, QEvent*) () from /usr/lib64/libQt5Core.so.5
#12 0x00007fff843b515 in QCOREApplicationPrivate::sendPostedEvents(QObject*, int, QThreadData*) () from /usr/lib64/libQt5Core.so.5
#13 0x00007fff843a9f373 in postEventSourceDispatch(_GSource*, int (void), void*) () from /usr/lib64/libQt5Core.so.5
#14 0x00007fff763b57 in g_main_context_dispatch () from /usr/lib64/libglib-2.0.so.0
#15 0x00007fff763d88 in ?? () from /usr/lib64/libglib-2.0.so.0
#16 0x00007fff763e1c in g_main_context_iteration () from /usr/lib64/libglib-2.0.so.0
#17 0x00007fff8439e9ef in QEventDispatcherGlib::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib64/libQt5Core.so.5
#18 0x00007fff843a4753a in QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) () from /usr/lib64/libQt5Core.so.5
#19 0x00007fff843f4d4c4 in QCOREApplication::exec() () from /usr/lib64/libQt5Core.so.5
#20 0x00005555555558189 in ?? ()
#21 0x00007fff730bc46a in __libc_start_main () from /lib64/libc.so.6
#22 0x0000555555555854a in __start ()

**History**

#1 - 28 Jul 2017 19:00 - Robin Mills
- Category set to not-a-bug
- Status changed from New to Assigned
- Assignee set to Robin Mills
- Target version set to 0.27
- % Done changed from 0 to 100
- Estimated time set to 1.00 h

I can't reproduce this with the exiv2(.exe) command line program on MacOS-X.

506 rmills@rmillsmbp:~/gnu/exiv2/0.26 $ exiv2 -pa ~/Downloads/IMG0006.JPG
Warning: Directory Pentax, entry 0x0004: Data area exceeds data buffer, ignoring it.
Error: XMP Toolkit error 203: Duplicate property or field node
Warning: Failed to decode XMP metadata.

Exif.Image.Make Ascii 19 PENTAX Corporation
Exif.Image.Model Ascii 17 PENTAX Optio M50

Exif.Thumbnail.XResolution Rational 1 72
Exif.Thumbnail.YResolution Rational 1 72
Exif.Thumbnail.ResolutionUnit Short 1 inch
Exif.Thumbnail.JPEGInterchangeFormat Long 1 5520
Exif.Thumbnail.JPEGInterchangeFormatLength Long 1 7564

507 rmills@rmillsmbp:/~gnu/exiv2/0.26 $ 
#2 - 29 Jul 2017 12:00 - Henri Salo
- File IMG0006-min.jpg added
With version 0.26 from http://exiv2.org/builds/exiv2-0.26-trunk.tar.gz
Build with: DFLAGS="-fsanitize=address" CXXFLAGS="-fsanitize=address -ggdb -fno-omit-frame-pointer" ./configure --enable-video --enable-webready

This file causes heap buffer overflow when executed using flag -pa. Without -pa flag no heap buffer overflow is detected.
258d54d0745e9958eb803da0d02cc45363f06d3b7e37268ff71d18c1e20fdd860 IMG0006.JPG
c3f8acd2496fc8f80ad6f730e363eb63d88377b2d80647a0ee78609c3b2b IMG0006-min.jpg

I have attached minimized sample file (using afl-2.49b/afl-tmin).

ASAn output is below:

afl@haiven2:/~exiv2-crashes$ ~/builds/exiv2/0.26-afl-asan/bin/exiv2 -pa IMG0006.JPG
Warning: Directory Pentax, entry 0x0004: Data area exceeds data buffer, ignoring it.
Error: XMP Toolkit error 203: Duplicate property or field node
Warning: Failed to decode XMP metadata.

Exif.Image.Make Ascii 19 PENTAX Corporation
Exif.Image.Model Ascii 17 PENTAX Optio M50
Exif.Image.Orientation Short 1 top, left
Exif.Image.XResolution Rational 1 72
Exif.Image.YResolution Rational 1 72
Exif.Image.ResolutionUnit Short 1 inch
Exif.Image.Software Ascii 12 GIMP 2.8.22
Exif.Image.YCbCrPositioning Short 1 Co-sited
Exif.Image.XIfTag Long 1 582
Exif.Photo.ExposureTime Rational 1 1/25 s
Exif.Photo.FNumber Rational 1 F3.5
Exif.Photo.ISOSpeedRatings Short 1 800
Exif.Photo.ExifVersion Undefined 4 2.20
Exif.Photo.DateTimeOriginal Ascii 20 2008:01:01 00:00:45
Exif.Photo.DateTimeDigitized Ascii 20 2008:01:01 00:00:45
Exif.Photo.ComponentsConfiguration Undefined 4 YCbCr
Exif.Photo.CompressedBitsPerPixel Rational 1 1
Exif.Photo.ExposureBiasValue SRational 1 0 EV
Exif.Photo.MaxApertureValue Rational 1 F3.5
Exif.Photo.MeteringMode Short 1 Multi-segment
Exif.Photo.FocalLength Rational 1 6.3 mm
Exif.Photo.MakerNote Undefined 4364 (Binary value suppressed)
Exif.MakerNote.Offset Long 1 1024
Exif.MakerNote.ByteOrder Ascii 3 II
Exif.Pentax.Version Byte 4 4.2.0.0
Exif.Pentax.PriorityResolution Short 2 640x480
Exif.Pentax.ResolutionUnit Long 1 38648
Exif.Pentax.PixelBlackLevel Long 1 15933
Exif.Pentax.PixelWhiteLevel Long 1 1 Optio M50
Exif.Pentax.Date Undefined 4 2008:01:01
Exif.Pentax.Time Undefined 3 00:00:45
Exif.Pentax.Quality Short 1 Better
Exif.Pentax.ResolutionUnit Short 1 inch
Exif.Pentax.Flash Short 1 Off, Did not fire
Exif.Pentax.Focus Short 1 Macro
Exif.Pentax.AFPoint Long 1 15933
Exif.Pentax.AFPointInFocus Short 1 Top-left
Exif.Pentax.ExposureTime   Long  1  38.97 ms
Exif.Pentax.FNumber        Short 1  F3.5
Exif.Pentax.ISO            Short 1  800
Exif.Pentax.ExposureCompensation Short 1  0 EV
Exif.Pentax.MeteringMode   Short 1  Multi Segment
Exif.Pentax.WhiteBalance   Short 1  Auto
Exif.Pentax.WhiteBalanceMode Short 1  Auto (Flash)
Exif.Pentax.BlueBalance    Short 1  469
Exif.Pentax.RedBalance     Short 1  401
Exif.Pentax.FocalLength    Long 1 6.3 mm
Exif.Pentax.DigitalZoom    Short 1  100
Exif.Pentax.Saturation     Short 1  Normal
Exif.Pentax.Contrast       Short 1  Normal
Exif.Pentax.Sharpness      Short 1  Normal
Exif.Pentax.Location       Short 1  Home town
Exif.Pentax.Hometown       Short 1  New York
Exif.Pentax.Destination    Short 1  New York
Exif.Pentax.HometownDST    Short 1  No
Exif.Pentax.DestinationDST Short 1  No
Exif.Pentax.DSPFirmwareVersion Undefined 4  254 255 255 255
Exif.Pentax.ImageProcessing Undefined 4 Unprocessed

1202ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000077b4 at pc 0x7e2167a3708 bp 0x7fcd49ce0 sp 0x7fcd49ce98
READ of size 4 at 0x602000077b4 thread T0 here:
#0 0x7e2167a3707 in Exiv2::ValueType<unsigned int>::toLong(long) const ../include/exiv2/value.hpp:1659
#4 0x7e21692bde7 in Exiv2::Internal::PentaxMakerNote::printShutterCount(std::ostream&, Exiv2::Value const&, Exiv2::ExifData const*) /home/afl/src/exiv2-trunk/src/metadatum.cpp:1193
#5 0x7e2167a3bea in Exiv2::Internal::PentaxMakerNote::print(std::ostream&, Exiv2::ExifData const*) /home/afl/src/exiv2-trunk/src/metadatum.cpp:38
#6 0x7e2167a3bea in Exiv2::Internal::PentaxMakerNote::print(Exiv2::ExifData const*) /home/afl/src/exiv2-trunk/src/metadatum.cpp:38
#7 0x7e2167a3bea in Exiv2::Internal::PentaxMakerNote::print(Exiv2::ExifData const*) /home/afl/src/exiv2-trunk/src/metadatum.cpp:38
#8 0x7e2167a3bea in Exiv2::Internal::PentaxMakerNote::print(Exiv2::ExifData const*) /home/afl/src/exiv2-trunk/src/metadatum.cpp:38
#9 0x7e2167a3bea in Exiv2::Internal::PentaxMakerNote::print(Exiv2::ExifData const*) /home/afl/src/exiv2-trunk/src/metadatum.cpp:38
#10 0x7e2167a3bea in Exiv2::Internal::PentaxMakerNote::print(Exiv2::ExifData const*) /home/afl/src/exiv2-trunk/src/metadatum.cpp:38
#11 0x7e2167a3bea in Exiv2::Internal::PentaxMakerNote::print(Exiv2::ExifData const*) /home/afl/src/exiv2-trunk/src/metadatum.cpp:38
#12 0x7e2167a3bea in Exiv2::Internal::PentaxMakerNote::print(Exiv2::ExifData const*) /home/afl/src/exiv2-trunk/src/metadatum.cpp:38

allocated by thread T0 here:
#0 0x7e2167a3bea in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.1+0x54fff)
#1 0x7e2167a3bea in __gnu_cxx::new_allocator<unsigned int>::allocate(unsigned long, void const*) /usr/include/c++/4.9/ext/new_allocator.h:104
#2 0x7e2167a3bea in Vector_base<unsigned int, std::allocator<unsigned int> >::assign(unsigned int const&) /usr/include/c++/4.9/ext/alloc_traits.h:182
#3 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::insert_node<typename _M_hasher>::_M_insert_node(Native_type const&):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#4 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#5 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#6 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#7 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#8 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#9 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#10 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#11 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#12 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#13 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#14 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#15 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
#16 0x7e2167a3bea in std::vector<unsigned int, std::allocator<unsigned int> >::push_back(unsigned int):
/usr/include/c++/4.9/ext/alloc_traits.h:182
SUMMARY: AddressSanitizer: heap-buffer-overflow ../include/exiv2/value.hpp:1659 Exiv2::ValueType<unsigned int>::toLong(long) const
Shadow bytes around the buggy address:
0x0c047fff8ea0: fa fa fd fd fa fa fa fa fa fa fa fa fa fa
0x0c047fff8eb0: fa fa fd fd fa fa fa fa fa fa fa fa fa fa
0x0c047fff8ec0: fa fa fd fd fa fa fa fa fa fa fa fa fa fa
0x0c047fff8ed0: fa fa fd fd fa fa fa fa fa fa fa fa fa fa
0x0c047fff8ee0: fa fa fd fd fa fa fa fa fa fa fa fa fa fa
0x0c047fff8ef0: fa fa fd fd fa fa
=>0x0c047fff8f00: fa fa fd fd fa fa fa fa fa fa fa fa fa fa
0x0c047fff8f10: fa fa fd fd fa fa fa fa fa fa fa fa fa fa
0x0c047fff8f20: fa fa fd fd fa fa fa fa fa fa fa fa fa fa
0x0c047fff8f30: fa fa fd fd fa fa fa fa fa fa fa fa fa fa
0x0c047fff8f40: fa fa fd fd 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
Contiguous container OOB:fc
ASan internal:           fe
12028ABORTING

The file was caused by a heap buffer overflow when executed using flag -pa. Without -pa flag no heap buffer overflow is detected.

I have attached minimized sample file (using afl-2.49b/afl-tmin).

ASan output is below:

```
af1@haiven2:/~/exiv2-crashes$ ~/builds/exiv2/0.26-trunk.tar.gz
Building with: DFLAGS="-fsanitize-address" CCXFLAGS="-fsanitize-address -ggdb -fno-omit-frame-pointer" ./configure --enable-video --enable-webrtc
This file causes heap buffer overflow when executed using flag -pa. Without -pa flag no heap buffer overflow is detected.
258d54d0745e9958eb803da602cc45363f06dd3b7e37268f11d181ce20fdd8e60 IMGPG0006.JPG
c3f8acdb496fc8f80ad67f30e363eb6ddfffe77353d31440047a0e67e68069c2b IMGPG0006-min.jpg
```

I have attached minimized sample file (using afl-2.49b/afl-tmin).

ASAn output is below:

```
af1@haiven2:/~/exiv2-crashes$ ~/builds/exiv2/0.26-trunk/bin/exiv2 --pa IMGPG0006.JPG
Warning: Directory Pentax, entry 0x0004: Data area exceeds data buffer, ignoring it.
Error: XMP Toolkit error 203: Duplicate property or field node
```

The file was caused by a heap buffer overflow when executed using flag -pa. Without -pa flag no heap buffer overflow is detected.

I have attached minimized sample file (using afl-2.49b/afl-tmin).

ASAn output is below:

```
af1@haiven2:/~/exiv2-crashes$ ~/builds/exiv2/0.26-trunk/bin/exiv2 --pa IMGPG0006.JPG
Warning: Directory Pentax, entry 0x0004: Data area exceeds data buffer, ignoring it.
Error: XMP Toolkit error 203: Duplicate property or field node
```

I have attached minimized sample file (using afl-2.49b/afl-tmin).

ASAn output is below:

```
af1@haiven2:/~/exiv2-crashes$ ~/builds/exiv2/0.26-trunk/bin/exiv2 --pa IMGPG0006.JPG
Warning: Directory Pentax, entry 0x0004: Data area exceeds data buffer, ignoring it.
Error: XMP Toolkit error 203: Duplicate property or field node
```

The file was caused by a heap buffer overflow when executed using flag -pa. Without -pa flag no heap buffer overflow is detected.

I have attached minimized sample file (using afl-2.49b/afl-tmin).

ASAn output is below:

```
af1@haiven2:/~/exiv2-crashes$ ~/builds/exiv2/0.26-trunk/bin/exiv2 --pa IMGPG0006.JPG
Warning: Directory Pentax, entry 0x0004: Data area exceeds data buffer, ignoring it.
Error: XMP Toolkit error 203: Duplicate property or field node
```

The file was caused by a heap buffer overflow when executed using flag -pa. Without -pa flag no heap buffer overflow is detected.

I have attached minimized sample file (using afl-2.49b/afl-tmin).

ASAn output is below:

```
af1@haiven2:/~/exiv2-crashes$ ~/builds/exiv2/0.26-trunk/bin/exiv2 --pa IMGPG0006.JPG
Warning: Directory Pentax, entry 0x0004: Data area exceeds data buffer, ignoring it.
Error: XMP Toolkit error 203: Duplicate property or field node
```

The file was caused by a heap buffer overflow when executed using flag -pa. Without -pa flag no heap buffer overflow is detected.

I have attached minimized sample file (using afl-2.49b/afl-tmin).

ASAn output is below:

```
af1@haiven2:/~/exiv2-crashes$ ~/builds/exiv2/0.26-trunk/bin/exiv2 --pa IMGPG0006.JPG
Warning: Directory Pentax, entry 0x0004: Data area exceeds data buffer, ignoring it.
Error: XMP Toolkit error 203: Duplicate property or field node
```
SUMMARY: AddressSanitizer: heap-buffer-overflow../include/exiv2/value.hpp:1659 Exiv2::ValueType<unsigned int>

Shadow bytes around the buggy address:
0x07fe21681ba4 in Exiv2::ExifDataType::ExifDataType(Exiv2::ExifDataType const&) /home/afl/src/exiv2-trunk/src/exif.cpp:211
0x07fe21681ba1 in Exiv2::ExifDataType::ExifDataType(Exiv2::ExifDataType const*, Exiv2::Value const*) /home/afl/src/exiv2-trunk/src/exif.cpp:571
Thanks for providing a lot more information about this issue. I'm on vacation at the moment and will investigate when I get home next week.

The function `PentaxMakerNote::printShutterCount` is missing a null check for the parameter `ExifData* metadata`. Gwenview uses `operator<<(std::ostream& os, const Metadatum& md)` to get metadata values, and with this operator the pointer is always null.

Are you saying that the fix is:

```cpp
std::ostream& PentaxMakerNote::printShutterCount(std::ostream& os, const Value& value, const ExifData* metadata)
{
    if (!metadata) return os;
    ExifData::const_iterator dateIt = metadata->findKey(ExifKey("Exif.PentaxDng.Date"));
    ...
}
```

I don't know whether it's better to return the untouched stream, to put "undefined" or to put the raw value without decoding it, but basically yes, that's the fix.

Right. Thank You very much for working on this and discovering the "core" of the issue. I think you are correct, we should do something like `return os << "undefined"`;

I hope to submit the fix today.

Thanks again for your help.
#9 - 12 Sep 2017 08:17 - Robin Mills
- % Done changed from 80 to 100
- Estimated time changed from 2.00 h to 8.00 h

Fix submitted to https://github.com/Exiv2/exiv2 5405d61

#10 - 12 Sep 2017 08:18 - Robin Mills
- Status changed from Assigned to Closed

Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Size</th>
<th>Date</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMGP0006.JPG</td>
<td>175 KB</td>
<td>28 Jul 2017</td>
<td>Anonymous</td>
</tr>
<tr>
<td>IMGP0006-min.jpg</td>
<td>12.1 KB</td>
<td>29 Jul 2017</td>
<td>Henri Salo</td>
</tr>
<tr>
<td>IMGP0006-min.jpg</td>
<td>12.1 KB</td>
<td>29 Jul 2017</td>
<td>Henri Salo</td>
</tr>
</tbody>
</table>