Exiv2 - Bug #619

Segfault when opening PNG image

09 Mar 2009 12:52 - Łukasz Krzyżak

Status:	Closed	**Start date:**	09 Mar 2009
Priority:	Normal	**Due date:**	
Assignee:	Andreas Huggel	**% Done:**	100%
Category:	basicio	**Estimated time:**	0.00 hour
Target version:	0.18.1		

Description

Hello
When trying to open one of my photos (made by some version of UFRaw) exiv2 crashes. I've found it in digikam stacktrace and then reproduced it with command line exiv2.

```
exiv2 -V

exiv2 0.18
```

stacktrace from gdb:

```
(gdb) set args -v -pa  Pictures/dsc_3908.png
(gdb) run
Starting program: /usr/bin/exiv2 -v -pa  Pictures/dsc_3908.png
File 1/1: Pictures/dsc_3908.png

Program received signal SIGSEGV, Segmentation fault.
Exiv2::Internal::PngChunk::readRawProfile (text=@0x7fffa431c3c0) at pngchunk.cpp:627
627     pngchunk.cpp: No such file or directory.
        in pngchunk.cpp
(gdb) bt
#0  Exiv2::Internal::PngChunk::readRawProfile (text=@0x7fffa431c3c0) at pngchunk.cpp:627
#1  0x00007f909be48991 in Exiv2::Internal::PngChunk::parseChunkContent (pImage=0x1585e50, key=<val
ue optimized out>,
    arr={pData_ = 0x7fffa431c3c0 "", size_ = 0}) at pngchunk.cpp:236

#2  0x00007f909be49a04 in Exiv2::Internal::PngChunk::decodeTXTChunk (pImage=0x1585e50, data=@0x7ff
fa431c430,
    type=Exiv2::Internal::PngChunk::tEXt_Chunk) at pngchunk.cpp:103

#3  0x00007f909be47b93 in Exiv2::PngImage::readMetadata (this=0x1585e50) at pngimage.cpp:147

#4  0x0000000000416907 in Action::Print::printList (this=0x1585ba0) at actions.cpp:637

#5  0x000000000041e375 in Action::Print::run (this=0x1585ba0, path=@0x1585860) at actions.cpp:228

#6  0x0000000000409da0 in main (argc=<value optimized out>, argv=0x628a40) at exiv2.cpp:165

(gdb) bt full

#0  Exiv2::Internal::PngChunk::readRawProfile (text=@0x7fffa431c3c0) at pngchunk.cpp:627

        info = {pData_ = 0x0, size_ = 0}

        i = <value optimized out>

        dp = <value optimized out>

        sp = 0x1 <Address 0x1 out of bounds>

        length = <value optimized out>
```

```
        unhex = '\0' <repeats 49 times>, "\001\002\003\004\005\006\a\b\t", '\0' <repeats 39 times>
, "\n\v\f\r\016\017"
#1  0x00007f909be48991 in Exiv2::Internal::PngChunk::parseChunkContent (pImage=0x1585e50, key=<val
ue optimized out>,
    arr={pData_ = 0x7fffa431c3c0 "", size_ = 0}) at pngchunk.cpp:236

        exifData = {pData_ = 0x0, size_ = 22568774}

        length = <value optimized out>

        exifHeader = "Exif\000"

#2  0x00007f909be49a04 in Exiv2::Internal::PngChunk::decodeTXTChunk (pImage=0x1585e50, data=@0x7ff
fa431c430,
    type=Exiv2::Internal::PngChunk::tEXt_Chunk) at pngchunk.cpp:103

        key = {pData_ = 0x1585f50 "Raw profile type exif", size_ = 21}

        arr = {pData_ = 0x0, size_ = 0}

#3  0x00007f909be47b93 in Exiv2::PngImage::readMetadata (this=0x1585e50) at pngimage.cpp:147

        cdataBuf = {pData_ = 0x1585f30 "Raw profile type exif", size_ = 22}

        bufRead = 22

        dataOffset = <value optimized out>

        closer = {bio_ = @0x1585bc0}

        cheaderBuf = {pData_ = 0x1585f10 "", size_ = 8}
```

I'm using Gentoo on x86_64 arch. Exiv was compiled with -march=native -O1 -ggdb -pipe flags.

Associated revisions

Revision 1763 - 12 Mar 2009 02:15 - Andreas Huggel

#619: Check for empty buffer. Fixes crash with some PNG images. (Lukasz Krzyzak)

History

#1 - 09 Mar 2009 14:37 - Łukasz Krzyżak

- File bug619.diff added

and a quick and very dirty fix...

#2 - 12 Mar 2009 08:14 - Andreas Huggel

- Category set to basicio

- Status changed from New to Resolved

- Assignee set to Andreas Huggel

- Target version set to 0.18.1

- % Done changed from 0 to 100

Thanks for reporting the issue and your patch! I've changed it only slightly to test the size of the buffer instead of the data pointer, as pointd out by Gilles.

#3 - 30 Mar 2009 06:13 - Andreas Huggel

- Status changed from Resolved to Closed

Files

dsc_3908.png	2.66 MB	09 Mar 2009	Łukasz Krzyżak
bug619.diff	573 Bytes	09 Mar 2009	Łukasz Krzyżak