Exiv2 - Bug #520

crash when loading certain image

19 Jun 2007 00:23 - Christian Weiske

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Andreas Huggel	**% Done:**	0%
Category:	exif	**Estimated time:**	0.00 hour
Target version:	0.15		

Description

I always get a crash when trying to load images shot with a certain digital camera.

You can repeat it by downloading http://tmp.cweiske.de/kaputt-exiv2.jpg and doing "exiv2 kaputt-exiv2.jpg" on command line.

Additional information:

gdb `which exiv2`
(gdb) run kaputtFotos2007\ 124.jpg
Starting program: /usr/bin/exiv2 kaputtFotos2007\ 124.jpg
(no debugging symbols found)...(no debugging symbols found)...(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...(no debugging symbols found)...Warning: Makernote tag 0xfe7f has invalid Exif type 65518; using 7 (undefined).
Warning: Makernote tag 0x5000 has invalid Exif type 1058; using 7 (undefined).
Warning: Makernote tag 0x8255 has invalid Exif type 15500; using 7 (undefined).
terminate called after throwing an instance of 'std::length_error'
what(): basic_string::_S_create

Program received signal SIGABRT, Aborted.
0xb7f2c410 in ?? ()
(gdb) bt
#0 0xb7f2c410 in ?? ()
#1 0xbf99752c in ?? ()
#2 0x00000006 in ?? ()
#3 0x00003b79 in ?? ()
#4 0xb7c0a6b1 in raise () from /lib/libc.so.6
#5 0xb7c0bde8 in abort () from /lib/libc.so.6
#6 0xb7deb220 in *__gnu_cxx::*_verbose_terminate_handler() () from /usr/lib/gcc/i686-pc-linux-gnu/4.1.2/libstdc++.so.6
#7 0xb7de8ce5 in std::set_unexpected(void (**)()) () from **/usr/lib/gcc/i686-pc-linux-gnu/4.1.2/libstdc++.so.6**
#8 0xb7de8d22 in std::terminate() () from /usr/lib/gcc/i686-pc-linux-gnu/4.1.2/libstdc++.so.6
#9 0xb7de8e5a in __cxa_throw () from /usr/lib/gcc/i686-pc-linux-gnu/4.1.2/libstdc++.so.6
***#10 0xb7d81bef in std::*_throw_length_error(char const**) () from /usr/lib/gcc/i686-pc-linux-gnu/4.1.2/libstdc++.so.6
#11 0xb7dc5370 in std::string::_Rep::_S_create(unsigned, unsigned, std::allocator<char> const&) ()
from /usr/lib/gcc/i686-pc-linux-gnu/4.1.2/libstdc++.so.6
#12 0xb7dc60f9 in std::string::_S_copy_chars(char*, *__gnu_cxx::*_normal_iterator<char*, std::string>, *__gnu_cxx::*
_normal_iterator<char*, std::string>) () from /usr/lib/gcc/i686-pc-linux-gnu/4.1.2/libstdc++.so.6
#13 0xb7dc6211 in std::string::string(char const*, unsigned, std::allocator<char> const&) ()
from /usr/lib/gcc/i686-pc-linux-gnu/4.1.2/libstdc++.so.6
#14 0xb7eec5b2 in Exiv2::StringValueBase::read(unsigned char const*, long, Exiv2::ByteOrder) () from /usr/lib/libexiv2.so.0
#15 0xb7e8fa28 in Exiv2::Exifdatum::setValue(Exiv2::Entry const&, Exiv2::ByteOrder) () from /usr/lib/libexiv2.so.0
#16 0xb7e8fb11 in Exiv2::Exifdatum::Exifdatum(Exiv2::Entry const&, Exiv2::ByteOrder) () from /usr/lib/libexiv2.so.0
#17 0xb7e94196 in Exiv2::ExifData::add(*__gnu_cxx::*_normal_iterator<Exiv2::Entry const*, std::vector<Exiv2::Entry,
std::allocator<Exiv2::Entry>---Type <return> to continue, or q <return> to quit---
> >, *__gnu_cxx::*_normal_iterator<Exiv2::Entry const*, std::vector<Exiv2::Entry, std::allocator<Exiv2::Entry> > >, Exiv2::ByteOrder) ()
from /usr/lib/libexiv2.so.0
#18 0xb7e947ae in Exiv2::ExifData::load(unsigned char const*, long) () from /usr/lib/libexiv2.so.0
#19 0xb7eac867 in Exiv2::JpegBase::readMetadata() () from /usr/lib/libexiv2.so.0
#20 0x080564d1 in std::string Exiv2::toString<int>(int const&) ()
#21 0x0805e55c in std::string Exiv2::toString<int>(int const&) ()
#22 0x080506c1 in ?? ()
#23 0xb7bf7838 in __libc_start_main () from /lib/libc.so.6
#24 0x0804b391 in ?? ()

Related issues:	
Is duplicate of Exiv2 - Bug #513: Sony Makernote crashes exiv2	**Closed**

History

#1 - 19 Jun 2007 02:14 - Andreas Huggel

Appears to be a duplicate of bug #513, which was fixed with r1106 (and 1124).

Please reopen if it still happens with the current version from SVN.

(I can't reproduce the crash with the SVN version of exiv2 here.)