Exiv2 - Bug #1089

single 0-byte exif comment leads to SIGABRT (134)

29 May 2015 23:20 - Felix Bolte

Status:	Closed	**Start date:**	29 May 2015
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	exif	**Estimated time:**	1.00 hour
Target version:	0.26		

Description

after some fuzzing with afl, a bug showed up when listing exif data (after setting an XPComment to a single 0-byte) due to a creation of a string with a size of -1:

```
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -p a ../makes_exiv2_fail.jpeg
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -M"set Exif.Image.XPComment 70" ~/afl-1.79b/tru
nk/makes_exiv2_fail.jpeg
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -p a ../makes_exiv2_fail.jpeg
Exif.Image.XPComment                         Byte        1  Warning: iconv: Invalid argument (errn
o = 22) inbytesleft = 1
70
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -M"set Exif.Image.XPComment 0" ~/afl-1.79b/trun
k/makes_exiv2_fail.jpeg
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -p a ../makes_exiv2_fail.jpeg
terminate called after throwing an instance of 'std::length_error'
  what():  basic_string::_S_create
Exif.Image.XPComment                         Byte        1  Aborted
felix@between:~/afl-1.79b/trunk/build$ echo $?
134
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -M"set Exif.Image.XPComment 70 0" ~/afl-1.79b/t
runk/makes_exiv2_fail.jpeg
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -p a ../makes_exiv2_fail.jpeg
Exif.Image.XPComment                         Byte        2  F
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -M"set Exif.Image.XPComment 70 0 70" ~/afl-1.79
b/trunk/makes_exiv2_fail.jpeg
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -p a ../makes_exiv2_fail.jpeg
Exif.Image.XPComment                         Byte        3  Warning: iconv: Invalid argument (errn
o = 22) inbytesleft = 1
70 0 70
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -M"set Exif.Image.XPComment 70 0 70 0" ~/afl-1.
79b/trunk/makes_exiv2_fail.jpeg
felix@between:~/afl-1.79b/trunk/build$ ./bin/exiv2 -p a ../makes_exiv2_fail.jpeg
Exif.Image.XPComment                         Byte        4  FF
[...]
```

i wrote a simple patch, which fixes this special case ... nevertheless the other question is, if the iconv warnings on odd bytes should be fixed as well or not?
so i wrote a second version which removes the last byte if it is an odd byte and improved the ucs-2 stripping of trailing 0-characters (btw: why are we doing that anyhow?) to iterate over the string multiple times ...

... please have a look if one of the patches (attached) is ok for you (i am not sure if v2 is necessary at all (e.g. if we are on windows without iconv))!

```
felix@between:~/afl-1.79b/trunk/build$ gdb -q ./bin/exiv2
Reading symbols from /home/felix/afl-1.79b/trunk/build/bin/exiv2...done.
(gdb) run -p a ../makes_exiv2_fail.jpeg
Starting program: /home/felix/afl-1.79b/trunk/build/bin/exiv2 -p a ../makes_exiv2_fail.jpeg
warning: no loadable sections found in added symbol-file system-supplied DSO at 0x7ffff7ffa000
terminate called after throwing an instance of 'std::length_error'
  what():  basic_string::_S_create
Exif.Image.XPComment                         Byte        1
Program received signal SIGABRT, Aborted.
```

```
0x00007ffff6f5d0d5 in __GI_raise (sig=<optimized out>) at ../nptl/sysdeps/unix/sysv/linux/raise.c:
64
64    ../nptl/sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0  0x00007ffff6f5d0d5 in __GI_raise (sig=<optimized out>) at ../nptl/sysdeps/unix/sysv/linux/rais
e.c:64
#1  0x00007ffff6f6083b in __GI_abort () at abort.c:91
#2  0x00007ffff75b269d in __gnu_cxx::__verbose_terminate_handler() () from /usr/lib/x86_64-linux-g
nu/libstdc++.so.6
#3  0x00007ffff75b0846 in ?? () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#4  0x00007ffff75b0873 in std::terminate() () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#5  0x00007ffff75b096e in __cxa_throw () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#6  0x00007ffff755d907 in std::__throw_length_error(char const*) () from /usr/lib/x86_64-linux-gnu
/libstdc++.so.6
#7  0x00007ffff7599aa2 in std::string::_Rep::_S_create(unsigned long, unsigned long, std::allocato
r<char> const&) () from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#8  0x00007ffff759b495 in char* std::string::_S_construct<char const*>(char const*, char const*, s
td::allocator<char> const&, std::forward_iterator_tag) () from /usr/lib/x86_64-linux-gnu/libstdc++
.so.6
#9  0x00007ffff759b61d in std::basic_string<char, std::char_traits<char>, std::allocator<char> >::
basic_string(char const*, unsigned long, std::allocator<char> const&) ()
   from /usr/lib/x86_64-linux-gnu/libstdc++.so.6
#10 0x00007ffff7a23d29 in Exiv2::Internal::printUcs2 (os=..., value=...) at /home/felix/afl-1.79b/
trunk/src/tags.cpp:2325
#11 0x00007ffff79b3804 in Exiv2::Exifdatum::write (this=0x6481b0, os=..., pMetadata=0x6499f0) at /
home/felix/afl-1.79b/trunk/src/exif.cpp:230
#12 0x00007ffff79dcd90 in Exiv2::Metadatum::print (this=0x6481b0, pMetadata=0x6499f0) at /home/fel
ix/afl-1.79b/trunk/src/metadatum.cpp:80
#13 0x000000000042ac0c in Action::Print::printMetadatum (this=0x649760, md=..., pImage=0x6499e0) a
t /home/felix/afl-1.79b/trunk/src/actions.cpp:711
#14 0x0000000000429a1f in Action::Print::printMetadata (this=0x649760, image=0x6499e0) at /home/fe
lix/afl-1.79b/trunk/src/actions.cpp:536
#15 0x0000000000429957 in Action::Print::printList (this=0x649760) at /home/felix/afl-1.79b/trunk/
src/actions.cpp:526
#16 0x0000000000426b05 in Action::Print::run (this=0x649760, path=...) at /home/felix/afl-1.79b/tr
unk/src/actions.cpp:241
#17 0x0000000000419c88 in main (argc=4, argv=0x7fffffffe258) at /home/felix/afl-1.79b/trunk/src/ex
iv2.cpp:171
```

Associated revisions

Revision 3986 - 11 Oct 2015 00:10 - Robin Mills

#1089. Thank You to Felix for reporting this and providing a patch.

History

#1 - 21 Aug 2015 17:58 - Robin Mills

- Status changed from New to Assigned

- Assignee set to Robin Mills

- Target version set to 0.26

#2 - 24 Sep 2015 11:10 - Robin Mills

- Estimated time set to 3.00 h

#3 - 11 Oct 2015 00:12 - Robin Mills

- Status changed from Assigned to Resolved

- % Done changed from 0 to 100

- Estimated time changed from 3.00 h to 1.00 h

Submitted: r3986 Thank You Felix for reporting this and for providing the patch.

I submitted your 0002 patch plus some cosmetic changes including detabbing the file.

To answer your question *"why are we skipping trailing null pairs?"*, the honest answer is *"I don't know because I didn't write the code!"*. However I

suspect that unconverted bytes are represented as null pairs and it might be better to remove them all, trailing or embedded. For now, I'm happy to accept your patch as it prevents the crash and makes the code more robust.

#4 - 06 Dec 2015 21:01 - Robin Mills

- Status changed from Resolved to Closed

I'm going to close this one. Thanks again to Felix for this contribution.

Files

0001-strip_ucs_only_if_size_bigger_equals_two.patch	847 Bytes	29 May 2015	Felix Bolte
0002-strip_ucs_only_if_size_bigger_equals_two_v2.patch	1.14 KB	29 May 2015	Felix Bolte