Exiv2 - Bug #1320

It is a heap-buffer-overflow in Exiv2::Jp2Image::readMetadata (jp2image.cpp:277)

23 Sep 2017 04:18 - Zhu Liu

Status:	Closed	**Start date:**	23 Sep 2017
Priority:	Normal	**Due date:**	
Assignee:	Robin Mills	**% Done:**	100%
Category:	exif	**Estimated time:**	1.00 hour
Target version:	0.27		

Description

I've submitted the vulnerability on bugzilla.redhat.com. the link is:https://bugzilla.redhat.com/show_bug.cgi?id=1494776

./exiv2 003-heap-buffer-over ==========
34506ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61200000be69 at pc 0x7fa4854c3935 bp 0x7ffdf8967ef0 sp 0x7ffdf8967698
READ of size 808464432 at 0x61200000be69 thread T0
#0 0x7fa4854c3934 in *_asan_memcpy (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x8c934)*
#1 0x7fa484d5f07c in Exiv2::Jp2Image::readMetadata() /root/fuzzing/exiv2-trunk/src/jp2image.cpp:277
#2 0x43ab02 in Action::Print::printSummary() /root/fuzzing/exiv2-trunk/src/actions.cpp:289
*#3 0x43a1af in Action::Print::run(std::*__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&)
/root/fuzzing/exiv2-trunk/src/actions.cpp:244
#4 0x422129 in main /root/fuzzing/exiv2-trunk/src/exiv2.cpp:170
#5 0x7fa4840a382f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#6 0x421af8 in _start (/usr/local/exiv2_ASAN/bin/exiv2+0x421af8)

0x61200000be69 is located 0 bytes to the right of 297-byte region [0x61200000bd40,0x61200000be69)
allocated by thread T0 here:
#0 0x7fa4854d06b2 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x996b2)
#1 0x454805 in Exiv2::DataBuf::DataBuf(long) /root/fuzzing/exiv2-trunk/include/exiv2/types.hpp:204
#2 0x7fa484d5ef9a in Exiv2::Jp2Image::readMetadata() /root/fuzzing/exiv2-trunk/src/jp2image.cpp:273
#3 0x43ab02 in Action::Print::printSummary() /root/fuzzing/exiv2-trunk/src/actions.cpp:289
#4 0x43a1af in Action::Print::run(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&)
/root/fuzzing/exiv2-trunk/src/actions.cpp:244
#5 0x422129 in main /root/fuzzing/exiv2-trunk/src/exiv2.cpp:170
#6 0x7fa4840a382f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 __asan_memcpy
Shadow bytes around the buggy address:
0x0c247fff9770: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c247fff9780: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c247fff9790: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c247fff97a0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
0x0c247fff97b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fff97c0: 00 00 00 00 00 00 00 00 00 00 00 00 00[01]fa fa
0x0c247fff97d0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
0x0c247fff97e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c247fff97f0: 00 00 00 00 00 00 00 00 00 00 00 01 fa fa fa fa
0x0c247fff9800: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c247fff9810: fa fa fa fa fa fa 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
Container overflow:      fc
Array cookie:            ac
Intra object redzone:    bb
ASan internal:           fe
34506ABORTING
```

History

#1 - 25 Sep 2017 19:03 - Robin Mills

- Assignee deleted (Robin Mills)

- Priority changed from Urgent to Normal

#2 - 18 Sep 2018 11:31 - Robin Mills

- Status changed from New to Closed

- Assignee set to Robin Mills

- % Done changed from 0 to 100

- Estimated time set to 1.00 h

Issue has been resolved on 'master' on both 'normal' and 'ASAN' builds:

```
792 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $ bin/exiv2 ~/Downloads/003-heap-buffer-over.dms
Exiv2 exception in print action for file /Users/rmills/Downloads/003-heap-buffer-over.dms:
corrupted image metadata
793 rmills@rmillsmbp:~/gnu/github/exiv2/exiv2/build $
```

Files

003-heap-buffer-over	7.45 KB	23 Sep 2017	Zhu Liu