

New issue

[Jump to bottom](#)

## heap-buffer-overflow write in Exiv2::Jp2Image::doWriteMetadata #1529

🔒 Closed

henices opened this issue on Apr 7, 2021 · 4 comments · Fixed by [#1534](#)

Assignees



Labels

security (crash)

Milestone

🏷️ v0.27.4

henices commented on Apr 7, 2021

## VERSION

exiv2 0.27.4.1

<https://github.com/Exiv2/exiv2/tree/0.27-maintenance>

## REPRODUCE

Compile exiv2 with asan:

```
CC=clang CXX=clang++ cmake .. -DCMAKE_BUILD_TYPE=Release -DCMAKE_CXX_FLAGS="-fsanitize=address" \
-DCMAKE_C_FLAGS="-fsanitize=address" -DCMAKE_EXE_LINKER_FLAGS="-fsanitize=address" \
-DCMAKE_MODULE_LINKER_FLAGS="-fsanitize=address"
```

Download testcases:

[https://github.com/henices/pocs/raw/master/tests\\_83a94b3337206caa6803f625eb63db061395cf14](https://github.com/henices/pocs/raw/master/tests_83a94b3337206caa6803f625eb63db061395cf14)

[https://github.com/henices/pocs/raw/master/tests\\_83a94b3337206caa6803f625eb63db061395cf14.exv](https://github.com/henices/pocs/raw/master/tests_83a94b3337206caa6803f625eb63db061395cf14.exv)

exiv2 in tests\_83a94b3337206caa6803f625eb63db061395cf14

```
=====
==4194247==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000f7 at pc 0x7f55bcfeed2d bp 0x7ffd0d945470 sp 0x7ffd0d945468
WRITE of size 8 at 0x602000000f7 thread T0
#0 0x7f55bcfeed2c in Exiv2::Jp2Image::doWriteMetadata(Exiv2::BasicIo&) (/home/henices/tests/exiv2/build_asan/lib/libexiv2.so.27+0x3b3d2c)
#1 0x7f55bcfec857 in Exiv2::Jp2Image::writeMetadata() (/home/henices/tests/exiv2/build_asan/lib/libexiv2.so.27+0x3b1857)
#2 0x541653 in (anonymous namespace)::metacopy(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>> > const&, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>> > const&, int, bool) (/home/henices/tests/exiv2/build_asan/bin/exiv2+0x541653)
#3 0x545049 in Action::Insert::run(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>> > const&)
(/home/henices/tests/exiv2/build_asan/bin/exiv2+0x545049)
#4 0x4fddf3 in main (/home/henices/tests/exiv2/build_asan/bin/exiv2+0x4fddf3)
#5 0x7f55bc6da1e1 in __libc_start_main /usr/src/debug/glibc-2.32-37-g760e1d2878/csu/../csu/libc-start.c:314:16
#6 0x4224cd in _start (/home/henices/tests/exiv2/build_asan/bin/exiv2+0x4224cd)

0x602000000f7 is located 5 bytes to the right of 2-byte region [0x602000000f0,0x602000000f2)
allocated by thread T0 here:
#0 0x4fad47 in operator new[](unsigned long) (/home/henices/tests/exiv2/build_asan/bin/exiv2+0x4fad47)
#1 0x7f55bd064606 in Exiv2::DataBuf::DataBuf(long) (/home/henices/tests/exiv2/build_asan/lib/libexiv2.so.27+0x429606)
#2 0x7f55bcfec857 in Exiv2::Jp2Image::writeMetadata() (/home/henices/tests/exiv2/build_asan/lib/libexiv2.so.27+0x3b1857)
#3 0x541653 in (anonymous namespace)::metacopy(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>> > const&, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>> > const&, int, bool) (/home/henices/tests/exiv2/build_asan/bin/exiv2+0x541653)
#4 0x545049 in Action::Insert::run(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>> > const&)
(/home/henices/tests/exiv2/build_asan/bin/exiv2+0x545049)
#5 0x4fddf3 in main (/home/henices/tests/exiv2/build_asan/bin/exiv2+0x4fddf3)
#6 0x7f55bc6da1e1 in __libc_start_main /usr/src/debug/glibc-2.32-37-g760e1d2878/csu/../csu/libc-start.c:314:16

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/henices/tests/exiv2/build_asan/lib/libexiv2.so.27+0x3b3d2c) in Exiv2::Jp2Image::doWriteMetadata(Exiv2::BasicIo&)
Shadow bytes around the buggy address:
 0x0c047fff7f7c: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c047fff8000: fa fa fd fa fa fd fa fa fd fa fa fd fa fa fd fa fa
=>0x0c047fff8010: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 02 fa
 0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff8060: 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
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
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
Left alloca redzone: ca
Right alloca redzone: cb
Shadow gap: cc
==4194247==ABORTING
```

Credit: Zhen Zhou of NSFOCUS Security Team

clanmills commented on Apr 8, 2021

Collaborator

Please provide your command-line to reproduce this issue.

I will fix this later today. I did intend to release Exiv2 v0.27.4 RC2 today. I will delay that for a few days to deal with anything else you discover in the next few days.

henices commented on Apr 8, 2021

Author

exiv2 in tests\_83a94b3337206caa6803f625eb63db061395cf14

clanmills commented on Apr 8, 2021


Collaborator

Thanks. I am now able to reproduce this. It will be fixed today.

```
559 rmills@rmillsmm-local:~/gnu/github/exiv2/0.27-maintenance/build/foo $ ls -l
total 88
```

```
-rw-r--r--@ 1 rmills staff 40609 8 Apr 08:01 tests_83a94b3337206caa6803f625eb63db061395cf14
-rw-r--r--@ 1 rmills staff 9 8 Apr 08:09 tests_83a94b3337206caa6803f625eb63db061395cf14.exv
560 rmills@rmillsmm-local:~/gnu/github/exiv2/0.27-maintenance/build/foo $ exiv2 in tests_83a94b3337206caa6803f625eb63db061395cf14
=====
==52084==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000001b7 at pc 0x00010525f7f4 bp 0x7ffeeab2ed10 sp 0x7ffeeab2ed08
WRITE of size 8 at 0x6020000001b7 thread T0
#0 0x10525f7f3 in Exiv2::Jp2Image::doWriteMetadata(Exiv2::BasicIo&)+0x2143 (libexiv2.0.27.4.2.dylib:x86_64+0xf27f3)
```


I will delay releasing Exiv2 v0.27.4 RC2 to deal with any other issues that your discover.

 **hassec** added help wanted labels on Apr 8, 2021

 **pydera** added a commit that referenced this issue on Apr 8, 2021

 Fix out of buffer access in [#1529](#)

✗ 3106ae5

 **pydera** added a commit that referenced this issue on Apr 8, 2021


 Fix out of buffer access in [#1529](#)

✓ 13e5a3e

 **clanmills** mentioned this issue on Apr 9, 2021

heap-buffer-overflow Read in Exiv2::Internal::CrwMap::encode [#1530](#)

 Closed


 **pydera** added a commit that referenced this issue on Apr 9, 2021

 Merge pull request [#1534](#) from Exiv2/fix\_1529 ...

✓ 0230620

 **pydera** closed this as completed on Apr 9, 2021

 **clanmills** assigned **pydera** on Apr 9, 2021

 **clanmills** added security (crash) and removed good first issue labels on Apr 9, 2021

 **clanmills** added this to the v0.27.4 milestone on Apr 9, 2021

 **clanmills** linked a pull request on Apr 9, 2021 that will close this issue

Fix out of buffer access in [#1529](#) [#1534](#)

 Merged

 **clanmills** mentioned this issue on Apr 9, 2021

Exiv2 RoadMap [#1018](#)

 Open

**fgeek** commented on Aug 6, 2021

[CVE-2021-31291](#) has been assigned for this issue.

#### Assignees

 **pydera**

#### Labels

security (crash)

#### Projects

None yet

#### Milestone

v0.27.4

#### Development

Successfully merging a pull request may close this issue.

 Fix out of buffer access in [#1529](#)  
Exiv2/exiv2

#### 5 participants

