<> Code ⊙ Issues 115 ⇅ Pull requests 18 💬 Discussions ▶ Actions ···

New issue

one global-buffer-overread in Exiv2::Internal::Nikon1MakerNote::print0x0088 in nikonmn_int.cpp #756

⊙ Closed **92wyunchao** opened this issue on Mar 24, 2019 · 2 comments · Fixed by #758

Labels   bug

92wyunchao commented on Mar 24, 2019 · edited by D4N ▾

POC:
poc.zip

There exists one global-buffer-overread in Exiv2::Internal::Nikon1MakerNote::print0x0088 in nikonmn_int.cpp in exiv2 0.27.99.0 which could result in information leak.

```
$ exiv2 -pt $poc

==27589==ERROR: AddressSanitizer: global-buffer-overflow on address 0xb7699d34 at pc 0xb6efa9f3 bp 0xbfc07508 sp 0xbfc07500
READ of size 4 at 0xb7699d34 thread T0
    #0 0xb6efa9f2 in Exiv2::Internal::Nikon1MakerNote::print0x0088(std::ostream&, Exiv2::Value const&, Exiv2::ExifData const*) /home/rookie/asan/exiv2-
master/src/nikonmn_int.cpp:374
    #1 0xb6677efc in Exiv2::Exifdatum::write(std::ostream&, Exiv2::ExifData const*) const /home/rookie/asan/exiv2-master/src/exif.cpp:227
    #2 0xb68d6c1c in Exiv2::Metadatum::print(Exiv2::ExifData const*) const /home/rookie/asan/exiv2-master/src/metadatum.cpp:74
    #3 0x82150ef in Action::Print::printMetadatum(Exiv2::Metadatum const&, Exiv2::Image const*) /home/rookie/asan/exiv2-master/src/actions.cpp:745
    #4 0x8206d2d in Action::Print::printMetadata(Exiv2::Image const*) /home/rookie/asan/exiv2-master/src/actions.cpp:542
    #5 0x81fabf1 in Action::Print::printList() /home/rookie/asan/exiv2-master/src/actions.cpp:531
    #6 0x81a6225 in Action::Print::run(std::string const&) /home/rookie/asan/exiv2-master/src/actions.cpp:248
    #7 0x80d3aa5 in main /home/rookie/asan/exiv2-master/src/exiv2.cpp:172
    #8 0xb600aaf2 (/lib/i386-linux-gnu/libc.so.6+0x19af2)
    #9 0x80d1af4 in _start (/home/rookie/asan/exiv2-master/build/bin/exiv2+0x80d1af4)

0xb7699d34 is located 44 bytes to the left of global variable 'Exiv2::Internal::nikonFlashControlMode' from '/home/rookie/asan/exiv2-master/src/nikonmn_int.cpp' (0xb7699d60) of
size 108
0xb7699d34 is located 76 bytes to the right of global variable 'Exiv2::Internal::nikonFlashGNDistance' from '/home/rookie/asan/exiv2-master/src/nikonmn_int.cpp' (0xb7699b20) of
size 456
SUMMARY: AddressSanitizer: global-buffer-overflow /home/rookie/asan/exiv2-master/src/nikonmn_int.cpp:374 Exiv2::Internal::Nikon1MakerNote::print0x0088(std::ostream&, Exiv2::Value
const&, Exiv2::ExifData const*)
Shadow bytes around the buggy address:
  0x36ed3350: 00 00 00 00 00 00 00 00 00 00 00 00 f9 f9 f9
  0x36ed3360: f9 f9 f9 f9 00 00 00 00 00 00 00 00 00 00 00
  0x36ed3370: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x36ed3380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x36ed3390: 00 00 00 00 00 00 00 00 00 00 00 00 f9 f9 f9
=>0x36ed33a0: f9 f9 f9 f9 f9 f9[f9]f9 f9 f9 f9 00 00 00 00
  0x36ed33b0: 00 00 00 00 00 00 00 04 f9 f9 f9 f9 f9 f9 f9
  0x36ed33c0: 00 00 00 00 04 f9 f9 f9 f9 f9 f9 00 00 00 00
  0x36ed33d0: 00 00 00 00 00 00 00 04 f9 f9 f9 f9 f9 f9 f9
  0x36ed33e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x36ed33f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
  ASan internal:         fe
==27589==ABORTING
```

🏷️ **D4N** added the bug label on Mar 25, 2019

D4N commented on Mar 25, 2019   Member

I can confirm that this bug is present on master, although you'll have to explain to me how this is an information leak.

⧉ **D4N** added a commit that referenced this issue on Mar 25, 2019

   ⬡ [tests] Add regression test for #756   7bd929d

⧉ **D4N** added a commit that referenced this issue on Mar 25, 2019

   ⬡ [tests] Add regression test for #756 ···   4e9990d

⧉ ⬡ **D4N** mentioned this issue on Mar 25, 2019

      Fix #756 #758

      ⑂ Merged

D4N commented on Mar 25, 2019   `Member`

This issue will get fixed by #757 and #758 for 0.27-maintenance and master, respectively.

D4N added a commit that referenced this issue on Mar 26, 2019

Merge pull request #757 from Exiv2/fix_756_0.27 ···   b148cfa

D4N added a commit that referenced this issue on Mar 29, 2019

[tests] Add regression test for #756 ···   417c755

clanmills pushed a commit that referenced this issue on Mar 29, 2019

[tests] Add regression test for #756   1a564a4

D4N closed this as completed in #758 on Mar 29, 2019

D4N added a commit that referenced this issue on Mar 29, 2019

Merge pull request #758 from Exiv2/fix_756 ···   476be79

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix #756
Exiv2/exiv2

2 participants