

New issue

Jump to bottom

one invalid memory access in decode function in iptc.cpp #760

Closed 92wyunchao opened this issue on Mar 25, 2019 · 2 comments

92wyunchao commented on Mar 25, 2019

POC:
[segment_poc.zip](#)

`gdb --args ./exiv2 -pt ~/segment_poc`


Program received signal SIGSEGV, Segmentation fault.
0xb7c649d6 in Exiv2::IptcParser::decode (iptcData=..., pData=, size=) at /home/rookie/exiv2-master/src/iptc.cpp:453
453 if (pRead++ != marker_) continue;
(gdb) bt
#0 0xb7c649d6 in Exiv2::IptcParser::decode (iptcData=..., pData=, size=) at /home/rookie/exiv2-master/src/iptc.cpp:453
#1 0xb7e49838 in Exiv2::Internal::TiffDecoder::decodeIptc (this=, object=0x0) at /home/rookie/exiv2-master/src/tiffvisitor_int.cpp:428
#2 0xb7e46726 in decodeTiffEntry (this=, object=) at /home/rookie/exiv2-master/src/tiffvisitor_int.cpp:476
#3 Exiv2::Internal::TiffDecoder::visitEntry (this=, object=) at /home/rookie/exiv2-master/src/tiffvisitor_int.cpp:312
#4 0xb7e28e2a in Exiv2::Internal::TiffEntry::doAccept (this=0x80cbf00, visitor=...) at /home/rookie/exiv2-master/src/tiffcomposite_int.cpp:895
#5 0xb7e2907a in operator (this=, visitor=..., this=) at /home/rookie/exiv2-master/src/tiffcomposite_int.cpp:890
#6 Exiv2::Internal::TiffDirectory::doAccept (this=, visitor=...) at /home/rookie/exiv2-master/src/tiffcomposite_int.cpp:918
#7 0xb7e28dae in Exiv2::Internal::TiffComponent::accept (this=0x80cbd40, visitor=...) at /home/rookie/exiv2-master/src/tiffcomposite_int.cpp:890
#8 0xb7e35f69 in Exiv2::Internal::TiffParserWorker::decode (exifData=..., iptcData=..., xmpData=..., pData=, size=, root=, findDecoderFct=, pHeader=) at /home/rookie/exiv2-master/src/tiffimage_int.cpp:1562
#9 0xb7cf54be in Exiv2::TiffImage::readMetadata (this=) at /home/rookie/exiv2-master/src/tiffimage.cpp:187
#10 0x0807e002 in Action::Print::printList (this=0x80cbb28) at /home/rookie/exiv2-master/src/actions.cpp:523
#11 0x08070c67 in Action::Print::run (this=0x80cbb28, path="/home/rookie/segment_poc") at /home/rookie/exiv2-master/src/actions.cpp:248
#12 0x0804dd9b in main (argc=, argv=) at /home/rookie/exiv2-master/src/exiv2.cpp:172

piponazo commented on Apr 7, 2019

Collaborator

I run your example in master and 0.27 without being able to reproduce the issue. I'm closing this issue for the moment.

If you still have the problem, please re-open the issue and provide more information about the the environment where you are having the problem.

 piponazo closed this as completed on Apr 7, 2019

92wyunchao commented on Apr 10, 2019 · edited

Author

I am sure this issue exists in the master branch , and I can reproduce it. I build it with default compiler option in Ubuntu 14.04 32bit system.

`$uname -a`
Linux ubuntu 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux

`$file exiv2`
exiv2: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.24, BuildID[sha1]=e27c0bc0964c1b11679036566647eb59cd11db68, not stripped

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants

