

[New issue](#)[Jump to bottom](#)

"LibRaw::parse_exif()" Out-of-bounds write vulnerability #301

[Closed](#)

GirIElecta opened this issue on Jun 15, 2020 · 1 comment

GirIElecta commented on Jun 15, 2020

Description

An out-of-bounds write vulnerability exists within the "LibRaw::parse_exif()" function (libraw\src\metadata\exif_gps.cpp) which can be triggered by changing the AtomName from "CMT1" to an unknown name and making the "tiff_nifds" field equals zero.

Steps to Reproduce

(poc archive password= girielecta).

https://drive.google.com/file/d/1ExYAqarMtdA_cpcvn2JFvYFP6QKKC5SN/view?usp=sharing

cmd:

magick.exe convert poc.cr3 new.png

Upon running this, following crash happens only in ImageMagick x64 (Note: I enabled page heap on magick.exe):

Microsoft (R) Windows Debugger Version 10.0.19041.1 AMD64

Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: C:\ImageMagick-7.0.10-x64\VisualMagick\bin\magick.exe convert e:\poc.cr3 e:\new.png

***** Path validation summary *****

Response Time (ms) Location

Deferred srv*

Symbol search path is: srv*

Executable search path is:

ModLoad: 00007ff7 92190000 00007ff7 921a2000 magick.exe

ModLoad: 00007ffc ef540000 00007ffc ef730000 ntdll.dll

ModLoad: 00007ffc d4d50000 00007ffc d4dc1000 C:\WINDOWS\System32\verifier.dll

Page heap: pid 0x1824: page heap enabled with flags 0x3.

ModLoad: 00007ffc ee860000 00007ffc ee912000 C:\WINDOWS\System32\KERNEL32.DLL

ModLoad: 00007ffc ec6a0000 00007ffc ec944000 C:\WINDOWS\System32\KERNELBASE.dll

ModLoad: 00007ffc ea2a0000 00007ffc ea32f000 C:\WINDOWS\SYSTEM32\apphelp.dll

ModLoad: 00007ffc d4d20000 00007ffc d4d42000 C:\WINDOWS\SYSTEM32\VCRUNTIME140D.dll

ModLoad: 00007ffc cb0f0000 00007ffc cb2ab000 C:\WINDOWS\SYSTEM32\ucrtbased.dll

ModLoad: 00007ffc c3650000 00007ffc c3942000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_MagickCore_dll

ModLoad: 00007ffc cae20000 00007ffc cafeb000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_MagickWand_dll

ModLoad: 00007ffc ee6c0000 00007ffc ee854000 C:\WINDOWS\System32\USER32.dll

ModLoad: 00007ffc ed510000 00007ffc ed531000 C:\WINDOWS\System32\win32u.dll

ModLoad: 00007ffc eebf0000 00007ffc eec16000 C:\WINDOWS\System32\GDI32.dll

ModLoad: 00007ffc ec500000 00007ffc ec694000 C:\WINDOWS\System32\gdi32full.dll

ModLoad: 00007ffc ecaa0000 00007ffc ecb3e000 C:\WINDOWS\System32\msvcvp_win.dll

ModLoad: 00007ffc ed330000 00007ffc ed42a000 C:\WINDOWS\System32\ucrtbase.dll

ModLoad: 00007ffc edce0000 00007ffc edd83000 C:\WINDOWS\System32\ADVAPI32.dll

ModLoad: 00007ffc eeda0000 00007ffc eee3e000 C:\WINDOWS\System32\msvcrt.dll

ModLoad: 00007ffc ef380000 00007ffc ef417000 C:\WINDOWS\System32\sechost.dll

ModLoad: 00007ffc ee450000 00007ffc ee570000 C:\WINDOWS\System32\RPCRT4.dll

ModLoad: 00007ffc ee580000 00007ffc ee5ef000 C:\WINDOWS\System32\WS2_32.dll

ModLoad: 00007ffc d4cf0000 00007ffc d4d17000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_bzlib_dll

ModLoad: 00007ffc cd6d0000 00007ffc cd756000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_lcms_dll

ModLoad: 00007ffc ca8d0000 00007ffc ca9ef000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_freetype_dll

ModLoad: 00007ffc cd600000 00007ffc cd6a0000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_libxml_dll

ModLoad: 00007ffc d2ed0000 00007ffc d2f05000 C:\WINDOWS\SYSTEM32\VCOMP140D.DLL

ModLoad: 00007ffc d4cc0000 00007ffc d4ce3000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_lqr_dll

ModLoad: 00007ffc d2790000 00007ffc d27ba000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_zlib_dll

ModLoad: 000001a2 eecce000 000001a2 eed0a000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_zlib_dll

ModLoad: 00007ffc c1460000 00007ffc c179b000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_glib_dll

ModLoad: 00007ffc ed5f0000 00007ffc edcd4000 C:\WINDOWS\System32\SHELL32.dll

ModLoad: 00007ffc ed2e0000 00007ffc ed32a000 C:\WINDOWS\System32\cfgmgr32.dll

ModLoad: 00007ffc eec20000 00007ffc eecc9000 C:\WINDOWS\System32\shcore.dll

ModLoad: 00007ffc eded0000 00007ffc ee260000 C:\WINDOWS\System32\combase.dll

ModLoad: 00007ffc ed430000 00007ffc ed4b0000 C:\WINDOWS\System32\bcryptPrimitives.dll

ModLoad: 00007ffc ecb40000 00007ffc ed2be000 C:\WINDOWS\System32\windows.storage.dll

ModLoad: 00007ffc ec450000 00007ffc ec473000 C:\WINDOWS\System32\profapi.dll

ModLoad: 00007ffc ec480000 00007ffc ec4ca000 C:\WINDOWS\System32\powrprof.dll

ModLoad: 00007ffc ec400000 00007ffc ec410000 C:\WINDOWS\System32\UMPDCL.dll

ModLoad: 00007ffc ee3f0000 00007ffc ee442000 C:\WINDOWS\System32\shlwapi.dll

ModLoad: 00007ffc ec410000 00007ffc ec421000 C:\WINDOWS\System32\kernel.appcore.dll

ModLoad: 00007ffc ed2c0000 00007ffc ed2d7000 C:\WINDOWS\System32\cryptsp.dll

ModLoad: 00007ffc ee210000 00007ffc ee367000 C:\WINDOWS\System32\ole32.dll

ModLoad: 00007ffc eb920000 00007ffc eb95a000 C:\WINDOWS\SYSTEM32\PHLPAPI.DLL

ModLoad: 00007ffc eb960000 00007ffc eba2b000 C:\WINDOWS\SYSTEM32\DNSAPI.dll

ModLoad: 00007ffc eed80000 00007ffc eed88000 C:\WINDOWS\System32\NSI.dll

(1824.1fc8): Break instruction exception - code 80000003 (first chance)

ntdll!LdrpDoDebuggerBreak+0x30:

00007ffc efb1119c cc int 3

0:000> g

ModLoad: 00007ffc eed50000 00007ffc eed7e000 C:\WINDOWS\System32\IMM32.DLL

ModLoad: 00007ffc e32a0000 00007ffc e32af000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\IM_MOD_DB_DNG_dll

ModLoad: 00007ffc c12b0000 00007ffc c145c000 C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_libraw_dll

ModLoad: 00007ffc ca700000 00007ffc ca7f6000 C:\WINDOWS\SYSTEM32\MSVCP140D.dll

(1824.1fc8): Access violation - code c0000005 (first chance)

First chance exceptions are reported before any exception handling.

This exception may be expected and handled.

*** WARNING: Unable to verify checksum for C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_libraw_dll

CORE_DB_libraw_ILibRaw::parse_exif+0xc21:

00007ffc c130f541 f30f1184012c900600 movss dword ptr [rcx+rax+6962Ch],xmm0 ds:00008412 f3b2d48c=????????

0:000> k

Child-Sp RetAddr Call Site

00 0000003f a10ef000 00007ffc c12f44ee CORE_DB_libraw_ILibRaw::parse_exif+0xc21 [c:\imagemagick-7.0.10-19-x64\libraw\src\metadata\exif_gps.cpp @ 121]

01 0000003f a10ef600 00007ffc c12f533d CORE_DB_libraw_ILibRaw::parseCR3+0x8fe [c:\imagemagick-7.0.10-19-x64\libraw\src\metadata\cr3_parser.cpp @ 334]

02 0000003f a10ef930 00007ffc c12f533d CORE_DB_libraw_ILibRaw::parseCR3+0x174d [c:\imagemagick-7.0.10-19-x64\libraw\src\metadata\cr3_parser.cpp @ 518]

03 0000003f a10efc00 00007ffc c12d0b5f CORE_DB_libraw_ILibRaw::parseCR3+0x174d [c:\imagemagick-7.0.10-19-x64\libraw\src\metadata\cr3_parser.cpp @ 518]

04 0000003f a10efd00 00007ffc c13a79de CORE_DB_libraw_ILibRaw::identify+0x2085 [c:\imagemagick-7.0.10-19-x64\libraw\src\metadata\identify.cpp @ 719]

05 0000003f a10f33f0 00007ffc c13ab149 CORE_DB_libraw_ILibRaw::open_datastream+0x10e [c:\imagemagick-7.0.10-19-x64\libraw\src\utils\open.cpp @ 377]

06 0000003f a10f3690 00007ffc c13bdfc8 CORE_DB_libraw_ILibRaw::open_file+0x269 [c:\imagemagick-7.0.10-19-x64\libraw\src\utils\open.cpp @ 99]

*** WARNING: Unable to verify checksum for C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\IM_MOD_DB_DNG_dll

07 0000003f a10f37c0 00007ffc e32a1983 CORE_DB_libraw_ILibRaw::open_wfile+0x58 [c:\imagemagick-7.0.10-19-x64\libraw\src\libraw_c_api.cpp @ 113]

*** WARNING: Unable to verify checksum for C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_MagickCore_dll

08 0000003f a10f3800 00007ffc c36c6c97 IM_MOD_DB_DNG_IReadDNGImage+0x2d3 [c:\imagemagick-7.0.10-19-x64\imagemagick\coders\dng.c @ 413]

09 0000003f a10f5910 00007ffc c36c84a3 CORE_DB_MagickCore_IReadImage+0x5e7 [c:\imagemagick-7.0.10-19-x64\imagemagick\magickcore\constitute.c @ 553]

*** WARNING: Unable to verify checksum for C:\ImageMagick-7.0.10-19-x64\VisualMagick\bin\CORE_DB_MagickWand_dll

0a 0000003f a10fab30 00007ffc cae5aac3 CORE_DB_MagickCore_IReadImages+0x393 [c:\imagemagick-7.0.10-19-x64\imagemagick\magickcore\constitute.c @ 943]

0b 0000003f a10fb000 00007ffc caef44ae CORE_DB_MagickWand_IConvertImageCommand+0x1523 [c:\imagemagick-7.0.10-19-x64\imagemagick\magickwand\convert.c @ 606]

*** WARNING: Unable to verify checksum for magick.exe

0c 0000003f a10fd730 00007ffc 921914ea CORE_DB_MagickWand_IMagickCommandGenesis+0x33e [c:\imagemagick-7.0.10-19-x64\imagemagick\magickwand\magrify.c @ 191]

0d 0000003f a10fe800 00007ffc 92191693 magick!MagickMain+0x4ea [c:\imagemagick-7.0.10-19-x64\imagemagick\utilities\magick.c @ 149]

0e 0000003f a10ff010 00007ffc 92191f24 magick!wmain+0x43 [c:\imagemagick-7.0.10-19-x64\imagemagick\utilities\magick.c @ 195]

0f 0000003f a10ff050 00007ffc 92191e37 magick!invoke_main+0x34 [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 80]

10 0000003f a10ff090 00007ffc 92191cfe magick!_scrt_common_main_seh+0x127 [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 253]

11 0000003f a10ff0f0 00007ffc 92191f39 magick!_scrt_common_main+0xe [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 296]

```
12 0000003f a10ffc20 00007ffc ee877bd4 magick!wmainCRTStartup+0x9 [f:\dd\vctools\crt\vcstartup\src\startup\exe_wmain.cpp @ 17]
13 0000003f a10ffc50 00007ffc ef5ace51 KERNEL32!BaseThreadInitThunk+0x14
14 0000003f a10ffc80 00000000 00000000 ntdll!RtlUserThreadStart+0x21
0:000> u
CORE_DB_libraw!LibRaw::parse_exif+0xc21 [c:\imagemagick-7.0.10-19-x64\libraw\src\metadata\exif_gps.cpp @ 121]:
00007ffc c130f541 f30f1184012c960600 movss dword ptr [rcx+rax+6962Ch],xmm0 00007ffc c130f54a e9080b0000 jmp CORE_DB_libraw!LibRaw::parse_exif+0x1737 (00007ffc c1310057)
00007ffc c130f54f 8b542474 mov edx,dword ptr [rsp+74h]
00007ffc c130f553 488b8c2400060000 mov rcx,qword ptr [rsp+600h] 00007ffc c130f55b e850ddfbff call CORE_DB_libraw!LibRaw::getreal (00007ffc c12cd2b0) 00007ffc c130f560 f20f5ac0 cvtsd2ss
xmm0,xmm0
00007ffc c130f564 488b842400060000 mov rax,qword ptr [rsp+600h] 00007ffc c130f56c f30f118018ef0200 movss dword ptr [rax+2EF18h],xmm0
```

System Configuration


- ImageMagick:
Version: ImageMagick-7.0.10-19-Q16 <https://imagemagick.org>
License: <https://imagemagick.org/script/license.php>
- Environment (Operating system, version and so on):
Distributor ID: Microsoft Windows
Description: Windows 10

  GirlELECTA changed the title ~~LibRaw "LibRaw::parse_exif()" Out-of-bounds write vulnerability~~ "LibRaw::parse_exif()" Out-of-bounds write vulnerability on Jun 15, 2020

LibRaw commented on Jun 16, 2020

Owner

great thanks, fixed in [55f0a0c](#)

 LibRaw closed this as completed on Jun 16, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

