LibRaw / **LibRaw** Public

Code Issues 1 Pull requests 1 Actions Projects Wiki ...

New issue

Jump to bottom

LibRaw "simple_decode_row()" Out-of-bounds read vulnerability #271

Closed **GirlElecta** opened this issue on Apr 2, 2020 · 3 comments

GirlElecta commented on Apr 2, 2020 • edited

Description

An out-of-bounds read vulnerability exists within the "simple_decode_row()" function (libraw\src\x3f\x3f_utils_patched.cpp) which can be triggered via an image with a large "row_stride" field.

Steps to Reproduce

(poc archive password= girlelecta):
https://drive.google.com/file/d/12pjib7aED6VFvV8jmZup_vmROmnchXSb/view

cmd:
magick.exe convert poc2.X3F new.png

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

```
Microsoft (R) Windows Debugger Version 10.0.18362.1 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\magick.exe convert E:\Workspace\poc2.X3F E:\Workspace\new.png
```

```
************* Path validation summary **************
Symbol search path is: srv*
Executable search path is:
ModLoad: 00007ff6 5a870000 00007ff6 5a882000 magick.exe
ModLoad: 00007ffe c1500000 00007ffe c16f0000 ntdll.dll
ModLoad: 00007ffe a7680000 00007ffe a76f1000 C:\WINDOWS\System32\verifier.dll
Page heap: pid 0x1228: page heap enabled with flags 0x3.
ModLoad: 00007ffe bf9a0000 00007ffe bfa52000 C:\WINDOWS\System32\KERNEL32.DLL
ModLoad: 00007ffe be510000 00007ffe be7b3000 C:\WINDOWS\System32\KERNELBASE.dll
ModLoad: 00007ffe 81c90000 00007ffe 81f19000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_MagickCore_.dll
ModLoad: 00007ffe 96450000 00007ffe 96619000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_MagickWand_.dll
ModLoad: 00007ffe c0ea0000 00007ffe c1034000 C:\WINDOWS\System32\USER32.dll
ModLoad: 00007ffe ade30000 00007ffe ade52000 C:\WINDOWS\SYSTEM32\VCRUNTIME140D.dll
ModLoad: 00007ffe bf580000 00007ffe bf5a1000 C:\WINDOWS\System32\win32u.dll
ModLoad: 00007ffe 92510000 00007ffe 926cb000 C:\WINDOWS\SYSTEM32\ucrtbased.dll
ModLoad: 00007ffe c0910000 00007ffe c0936000 C:\WINDOWS\System32\GDI32.dll
ModLoad: 00007ffe be7c0000 00007ffe be954000 C:\WINDOWS\System32\gdi32full.dll
ModLoad: 00007ffe beab0000 00007ffe beb4e000 C:\WINDOWS\System32\msvcp_win.dll
ModLoad: 00007ffe beb80000 00007ffe bec7a000 C:\WINDOWS\System32\ucrtbase.dll
ModLoad: 00007ffe c1280000 00007ffe c1323000 C:\WINDOWS\System32\ADVAPI32.dll
ModLoad: 00007ffe c0bb0000 00007ffe c0c4e000 C:\WINDOWS\System32\msvcrt.dll
ModLoad: 00007ffe c0cc0000 00007ffe c0d57000 C:\WINDOWS\System32\sechost.dll
ModLoad: 00007ffe c02a0000 00007ffe c03c0000 C:\WINDOWS\System32\RPCRT4.dll
ModLoad: 00007ffe a9270000 00007ffe a9297000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_bzlib_.dll
ModLoad: 00007ffe 9a830000 00007ffe 9a94f000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_freetype_.dll
ModLoad: 00007ffe a20e0000 00007ffe a2166000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_lcms_.dll
ModLoad: 00007ffe 9eea0000 00007ffe 9ef40000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_libxml_.dll
ModLoad: 00007ffe a8d20000 00007ffe a8d43000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_lqr_.dll
ModLoad: 00007ffe a8a60000 00007ffe a8a8a000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_zlib_.dll
ModLoad: 00007ffe 81950000 00007ffe 81c8b000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_glib_.dll
ModLoad: 00007ffe bfa60000 00007ffe c0145000 C:\WINDOWS\System32\SHELL32.dll
ModLoad: 00007ffe bf530000 00007ffe bf57a000 C:\WINDOWS\System32\cfgmgr32.dll
ModLoad: 00007ffe c0b00000 00007ffe c0ba9000 C:\WINDOWS\System32\shcore.dll
ModLoad: 00007ffe bf5b0000 00007ffe bf8e6000 C:\WINDOWS\System32\combase.dll
ModLoad: 00007ffe be490000 00007ffe be510000 C:\WINDOWS\System32\bcryptPrimitives.dll
ModLoad: 00007ffe c1430000 00007ffe c149f000 C:\WINDOWS\System32\WS2_32.dll
ModLoad: 00007ffe bec80000 00007ffe bf3ff000 C:\WINDOWS\System32\windows.storage.dll
ModLoad: 00007ffe be470000 00007ffe be48f000 C:\WINDOWS\System32\profapi.dll
ModLoad: 00007ffe be400000 00007ffe be44a000 C:\WINDOWS\System32\powrprof.dll
ModLoad: 00007ffe be3d0000 00007ffe be3e0000 C:\WINDOWS\System32\UMPDC.dll
ModLoad: 00007ffe c1220000 00007ffe c1272000 C:\WINDOWS\System32\shlwapi.dll
ModLoad: 00007ffe be3e0000 00007ffe be3f1000 C:\WINDOWS\System32\kernel.appcore.dll
ModLoad: 00007ffe bf510000 00007ffe bf527000 C:\WINDOWS\System32\cryptsp.dll
ModLoad: 00007ffe c1040000 00007ffe c1196000 C:\WINDOWS\System32\ole32.dll
ModLoad: 00007ffe bd950000 00007ffe bd98a000 C:\WINDOWS\SYSTEM32\IPHLPAPI.DLL
ModLoad: 00007ffe bd990000 00007ffe bda5a000 C:\WINDOWS\SYSTEM32\DNSAPI.dll
ModLoad: 00007ffe c0220000 00007ffe c0228000 C:\WINDOWS\System32\NSI.dll
(1228.1894): Break instruction exception - code 80000003 (first chance)
ntdll!LdrpDoDebuggerBreak+0x30:
00007ffe c15d121c cc int 3
0:000> g
ModLoad: 00007ffe c1400000 00007ffe c142e000 C:\WINDOWS\System32\IMM32.DLL
ModLoad: 00007ffe ba570000 00007ffe ba57f000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\IM_MOD_DB_DNG_.dll
ModLoad: 00007ffe 8b450000 00007ffe 8b5fb000 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_libraw_.dll
ModLoad: 00007ffe 982d0000 00007ffe 983c6000 C:\WINDOWS\SYSTEM32\MSVCP140D.dll
(1228.1894): 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 E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_libraw_.dll
CORE_DB_libraw_!simple_decode_row+0x161:
00007ffe 8b550b71 8b0481 mov eax,dword ptr [rcx+rax*4] ds:0000020f d2200cb0=????????
0:000> k
Child-SP RetAddr Call Site
00 0000001a a29230d0 00007ffe 8b5509fc CORE_DB_libraw_!simple_decode_row+0x161 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 1154]
01 0000001a a2923180 00007ffe 8b557d93 CORE_DB_libraw_!simple_decode+0x8c [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 1191]
02 0000001a a29231e0 00007ffe 8b557ac1 CORE_DB_libraw_!x3f_load_huffman_not_compressed+0x93 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 1424]
03 0000001a a2923220 00007ffe 8b557ecd CORE_DB_libraw_!x3f_load_huffman+0x2b1 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 1472]
04 0000001a a2923290 00007ffe 8b557768 CORE_DB_libraw_!x3f_load_image+0x12d [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 1514]
05 0000001a a29232f0 00007ffe 8b558504 CORE_DB_libraw_!x3f_load_data+0x88 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 2059]
06 0000001a a2923330 00007ffe 8b553628 CORE_DB_libraw_!LibRaw::x3f_load_raw+0x64 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\libraw\src\x3f\x3f_parse_process.cpp @ 579]
07 0000001a a2923420 00007ffe 8b55d358 CORE_DB_libraw_!LibRaw::unpack+0xc18 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\libraw\src\decoders\unpack.cpp @ 283]
*** WARNING: Unable to verify checksum for E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\IM_MOD_DB_DNG_.dll
08 0000001a a29235e0 00007ffe ba571989 CORE_DB_libraw_!libraw_unpack+0x48 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\libraw\src\libraw_c_api.cpp @ 136]
*** WARNING: Unable to verify checksum for E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_MagickCore_.dll
09 0000001a a2923620 00007ffe 81ce83b7 IM_MOD_DB_DNG_!ReadDNGImage+0x479 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\imagemagick\coders\dng.c @ 425]
0a 0000001a a2925730 00007ffe 81ce9af3 CORE_DB_MagickCore_!ReadImage+0x5e7 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\imagemagick\magickcore\constitute.c @ 553]
*** WARNING: Unable to verify checksum for E:\Workspace\imageMagick\ImageMagick-windows\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_MagickWand_.dll
0b 0000001a a292a950 00007ffe 9648aac3 CORE_DB_MagickCore_!ReadImages+0x393 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\imagemagick\magickcore\constitute.c @ 927]
0c 0000001a a292ba00 00007ffe 96523fe8 CORE_DB_MagickWand_!ConvertImageCommand+0x1523 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\imagemagick\magickwand\convert.c @ 606]
*** WARNING: Unable to verify checksum for magick.exe
0d 0000001a a292d550 00007ff6 5a8714ea CORE_DB_MagickWand_!MagickCommandGenesis+0x338 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-
16\imagemagick\magickwand\mogrify.c @ 185]
0e 0000001a a292e6c0 00007ff6 5a871693 magick!MagickMain+0x4ea [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\imagemagick\utilities\magick.c @ 149]
0f 0000001a a292f930 00007ff6 5a871f24 magick!wmain+0x43 [e:\workspace\imagemagick\imagemagick-windows\imagemagick-7.0.9-16\imagemagick\utilities\magick.c @ 195]
10 0000001a a292f970 00007ff6 5a871e37 magick!invoke_main+0x34 [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 80]
11 0000001a a292f9b0 00007ff6 5a871cfe magick!__scrt_common_main_seh+0x127 [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 253]
12 0000001a a292fa10 00007ff6 5a871f39 magick!__scrt_common_main+0xe [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 296]
13 0000001a a292fa40 00007ffe bf9b7bd4 magick!wmainCRTStartup+0x9 [f:\dd\vctools\crt\vcstartup\src\startup\exe_wmain.cpp @ 17]
14 0000001a a292fa70 00007ffe c156ced1 KERNEL32!BaseThreadInitThunk+0x14
15 0000001a a292faa0 00000000 00000000 ntdll!RtlUserThreadStart+0x21
```

System Configuration

- ImageMagick:
  Version: ImageMagick-7.0.9-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

LibRaw commented on Apr 2, 2020 Owner

Another strange stack trace: setCancelFlag is not called from x3f_dpq_interpolate_rg, please recheck your stack trace.

GirlElecta commented on Apr 2, 2020 • edited Author

Provided stack trace is exact result of using k command on windbg. Can you please run PoC on ImageMagick using command I provided in report?
You should be able to reproduce this easily hopefully with a better stack trace.
Let me know if you need my help, please.

LibRaw commented on Apr 4, 2020 Owner

fixed by `5ab45b0`

LibRaw closed this as completed on Apr 4, 2020

LibRaw mentioned this issue on Apr 4, 2020

Handling of broken data Kalpanika/x3f#116

Closed

GirlElecta changed the title ~~out-of-bounds read in libraw\src\x3f\x3f_utils_patched.cpp~~ **"simple_decode_row()" Out-of-bounds read vulnerability** on Jun 15, 2020

GirlElecta changed the title ~~"simple_decode_row()" Out-of-bounds read vulnerability~~ **LibRaw "simple_decode_row()" Out-of-bounds read vulnerability** on Jun 17, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants