Libraw "new_node()" Out-of-bounds Write Vulnerability #272

Closed **0xfoxone** opened this issue on Apr 3, 2020 · 1 comment

0xfoxone commented on Apr 3, 2020

Description

There is an out-of-bounds write vulnerability within the "new_node()" function (libraw\src\x3f\x3f_utils_patched.cpp).

Steps to Reproduce

poc (password: 0xfoxone):
https://drive.google.com/open?id=1SGItp-hBZXEgrPErI6URiRkqUOT5J9In

cmd:

```
magick.exe convert poc.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: C:\ImageMagick-7.0.9-16\VisualMagick\bin\magick.exe convert C:\poc.X3F C:\new.png
```

```
Symbol search path is: srv*
Executable search path is:
ModLoad: 00000000 00830000 00000000 00840000 magick.exe
ModLoad: 00007ffe 62840000 00007ffe 62a30000 ntdll.dll
ModLoad: 00000000 77260000 00000000 773fa000 ntdll.dll
ModLoad: 00000000 01200000 00000000 01271000 C:\WINDOWS\System32\verifier.dll
Page heap: pid 0x9210: page heap enabled with flags 0x3.
ModLoad: 00007ffe 60bc0000 00007ffe 60c15000 C:\WINDOWS\System32\wow64.dll
ModLoad: 00007ffe 60b40000 00007ffe 60bbd000 C:\WINDOWS\System32\wow64win.dll
(9210.8cf4): Break instruction exception - code 80000003 (first chance)
ntdll!LdrInitShimEngineDynamic+0x35c:
00007ffe 6291121c cc int 3 0:000> g ModLoad: 00000000 77250000 00000000 77259000 C:\WINDOWS\System32\wow64cpu.dll ModLoad: 00000000 71620000 00000000 71683000
C:\WINDOWS\SysWOW64\verifier.dll Page heap: pid 0x9210: page heap enabled with flags 0x3. ModLoad: 00000000 74b20000 00000000 74c00000 C:\WINDOWS\SysWOW64\KERNEL32.DLL ModLoad:
00000000 75500000 00000000 756fd000 C:\WINDOWS\SysWOW64\KERNELBASE.dll ModLoad: 00000000 70750000 00000000 7099e000 C:\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_MagickCore_.dll
ModLoad: 00000000 714b0000 00000000 71611000 C:\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_MagickWand_.dll ModLoad: 00000000 74ce0000 00000000 74e77000
C:\WINDOWS\SysWOW64\USER32.dll ModLoad: 00000000 75eb0000 00000000 75ec7000 C:\WINDOWS\SysWOW64\win32u.dll ModLoad: 00000000 70ff0000 00000000 71163000
C:\WINDOWS\SysWOW64\ucrtbased.dll ModLoad: 00000000 71490000 00000000 714ac000 C:\WINDOWS\SysWOW64\VCRUNTIME140D.dll ModLoad: 00000000 71460000 00000000 71488000
C:\WINDOWS\SysWOW64\VCOMP140D.DLL ModLoad: 00000000 76fe0000 00000000 77001000 C:\WINDOWS\SysWOW64\GDI32.dll ModLoad: 00000000 75d30000 00000000 75e8a000
C:\WINDOWS\SysWOW64\gdi32full.dll ModLoad: 00000000 77150000 00000000 771cc000 C:\WINDOWS\SysWOW64\msvcp_win.dll ModLoad: 00000000 76720000 00000000 7683f000
C:\WINDOWS\SysWOW64\ucrtbase.dll ModLoad: 00000000 75480000 00000000 754f9000 C:\WINDOWS\SysWOW64\ADVAPI32.dll ModLoad: 00000000 764a0000 00000000 7655f000
C:\WINDOWS\SysWOW64\msvcrt.dll ModLoad: 00000000 771d0000 00000000 77246000 C:\WINDOWS\SysWOW64\sechost.dll ModLoad: 00000000 77010000 00000000 770cb000
C:\WINDOWS\SysWOW64\RPCRT4.dll ModLoad: 00000000 74a30000 00000000 74a50000 C:\WINDOWS\SysWOW64\SspiCli.dll ModLoad: 00000000 74a20000 00000000 74a2a000
C:\WINDOWS\SysWOW64\CRYPTBASE.dll ModLoad: 00000000 765f0000 00000000 7664f000 C:\WINDOWS\SysWOW64\bcryptPrimitives.dll ModLoad: 00000000 71440000 00000000 7145e000 C:\ImageMagick-
7.0.9-16\VisualMagick\bin\CORE_DB_bzlib_.dll ModLoad: 00000000 70680000 00000000 70750000 C:\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_freetype_.dll ModLoad: 00000000 70f80000
00000000 70fe6000 C:\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_lcms_.dll ModLoad: 00000000 71390000 00000000 713aa000 C:\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_lqr_.dll
ModLoad: 00000000 70bb0000 00000000 70c2c000 C:\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_libxml_.dll ModLoad: 00000000 6fd60000 00000000 6ffee000 C:\ImageMagick-7.0.9-
16\VisualMagick\bin\CORE_DB_glib_.dll ModLoad: 00000000 75f20000 00000000 7649a000 C:\WINDOWS\SysWOW64\SHELL32.dll ModLoad: 00000000 76850000 00000000 7688b000
C:\WINDOWS\SysWOW64\cfgmgr32.dll ModLoad: 00000000 71360000 00000000 71381000 C:\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_zlib_.dll ModLoad: 00000000 76560000 00000000 765e4000
C:\WINDOWS\SysWOW64\shcore.dll ModLoad: 00000000 75840000 00000000 75ab5000 C:\WINDOWS\SysWOW64\combase.dll ModLoad: 00000000 769b0000 00000000 76f75000
C:\WINDOWS\SysWOW64\windows.storage.dll ModLoad: 00000000 74c50000 00000000 74c67000 C:\WINDOWS\SysWOW64\profapi.dll ModLoad: 00000000 74c90000 00000000 74cd3000
C:\WINDOWS\SysWOW64\powrprof.dll ModLoad: 00000000 75700000 00000000 7570d000 C:\WINDOWS\SysWOW64\UMPDC.dll ModLoad: 00000000 75ed0000 00000000 75f14000
C:\WINDOWS\SysWOW64\shlwapi.dll ModLoad: 00000000 766c0000 00000000 7671e000 C:\WINDOWS\SysWOW64\WS2_32.dll ModLoad: 00000000 74f10000 00000000 74f1f000
C:\WINDOWS\SysWOW64\kernel.appcore.dll ModLoad: 00000000 75e90000 00000000 75ea3000 C:\WINDOWS\SysWOW64\cryptsp.dll ModLoad: 00000000 75ac0000 00000000 75bb7000
C:\WINDOWS\SysWOW64\ole32.dll ModLoad: 00000000 74920000 00000000 74952000 C:\WINDOWS\SysWOW64\IPHLPAPI.DLL ModLoad: 00000000 74880000 00000000 74911000
C:\WINDOWS\SysWOW64\DNSAPI.dll ModLoad: 00000000 76840000 00000000`76847000 C:\WINDOWS\SysWOW64\NSI.dll
(9210.8cf4): WOW64 breakpoint - code 4000001f (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
ntdll_77260000!LdrInitShimEngineDynamic+0x6e2:
7730e9e2 cc int 3
0:000:x86> g
ModLoad: 75810000 75835000 C:\WINDOWS\SysWOW64\IMM32.DLL
ModLoad: 71430000 7143e000 C:\ImageMagick-7.0.9-16\VisualMagick\bin\IM_MOD_DB_DNG_.dll
ModLoad: 70520000 70674000 C:\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_libraw_.dll
ModLoad: 70320000 703d9000 C:\WINDOWS\SysWOW64\MSVCP140D.dll
(9210.8cf4): 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-7.0.9-16\VisualMagick\bin\CORE_DB_libraw_.dll
CORE_DB_libraw_!new_node+0x41:
705dbf21 c74208ffffffff mov dword ptr [edx+8],0FFFFFFFFh ds:002b:117d0000=????????
0:000:x86> k
ChildEBP RetAddr
00 00fa4198 705cab75 CORE_DB_libraw_!new_node+0x41 [c:\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 715]
01 00fa41bc 705e2f65 CORE_DB_libraw_!add_code_to_tree+0x75 [c:\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 736]
02 00fa41e8 705ed80d CORE_DB_libraw_!populate_true_huffman_tree+0x95 [c:\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 762]
03 00fa4234 705ec86e CORE_DB_libraw_!x3f_load_true+0x36d [c:\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 1334]
04 00fa4254 705ec28c CORE_DB_libraw_!x3f_load_image+0xbe [c:\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 1509]
05 00fa426c 705ecd80 CORE_DB_libraw_!x3f_load_data+0x6c [c:\imagemagick-7.0.9-16\libraw\src\x3f\x3f_utils_patched.cpp @ 2058]
06 00fa42e8 705e86f5 CORE_DB_libraw_!LibRaw::x3f_load_raw+0x50 [c:\imagemagick-7.0.9-16\libraw\src\x3f\x3f_parse_process.cpp @ 579]
07 00fa4464 705f0abc CORE_DB_libraw_!LibRaw::unpack+0xa25 [c:\imagemagick-7.0.9-16\libraw\src\decoders\unpack.cpp @ 282]
*** WARNING: Unable to verify checksum for C:\ImageMagick-7.0.9-16\VisualMagick\bin\IM_MOD_DB_DNG_.dll
08 00fa4470 71431be6 CORE_DB_libraw_!libraw_unpack+0x2c [c:\imagemagick-7.0.9-16\libraw\src\libraw_c_api.cpp @ 136]
*** WARNING: Unable to verify checksum for C:\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_MagickCore_.dll
09 00fa64c8 707b25a3 IM_MOD_DB_DNG_!ReadDNGImage+0x466 [c:\imagemagick-7.0.9-16\imagemagick\coders\dng.c @ 425]
0a 00fab5e0 707b3b2c CORE_DB_MagickCore_!ReadImage+0x543 [c:\imagemagick-7.0.9-16\imagemagick\magickcore\constitute.c @ 553]
*** WARNING: Unable to verify checksum for C:\ImageMagick-7.0.9-16\VisualMagick\bin\CORE_DB_MagickWand_.dll
0b 00fac624 714dd449 CORE_DB_MagickCore_!ReadImages+0x2fc [c:\imagemagick-7.0.9-16\imagemagick\magickcore\constitute.c @ 927]
0c 00fadb84 71548b4d CORE_DB_MagickWand_!ConvertImageCommand+0xd29 [c:\imagemagick-7.0.9-16\imagemagick\magickwand\convert.c @ 606]
*** WARNING: Unable to verify checksum for magick.exe
0d 00faec40 008313de CORE_DB_MagickWand_!MagickCommandGenesis+0x2cd [c:\imagemagick-7.0.9-16\imagemagick\magickwand\mogrify.c @ 185]
0e 00fafd74 00831626 magick!MagickMain+0x3de [c:\imagemagick-7.0.9-16\imagemagick\utilities\magick.c @ 149]
0f 00fafd94 00831d2e magick!wmain+0x46 [c:\imagemagick-7.0.9-16\imagemagick\utilities\magick.c @ 195]
10 00fafda8 00831c10 magick!invoke_main+0x1e [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 79]
11 00fafe00 00831abd magick!__scrt_common_main_seh+0x150 [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 253]
12 00fafe08 00831d48 magick!__scrt_common_main+0xd [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 296]
13 00fafe10 74b36359 magick!wmainCRTStartup+0x8 [f:\dd\vctools\crt\vcstartup\src\startup\exe_wmain.cpp @ 17]
WARNING: Stack unwind information not available. Following frames may be wrong.
14 00fafe20 772c7b74 KERNEL32!BaseThreadInitThunk+0x19
15 00fafe7c 772c7b44 ntdll_77260000!RtlGetAppContainerNamedObjectPath+0xe4
16 00fafe8c 00000000 ntdll_77260000!RtlGetAppContainerNamedObjectPath+0xb4
```

System Configuration

- ImageMagick version:
  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

0xfoxone closed this as completed on Apr 3, 2020

0xfoxone reopened this on Apr 3, 2020

LibRaw commented on Apr 4, 2020 Owner

Fixed by `11c4db2`

LibRaw closed this as completed on Apr 4, 2020

0xfoxone changed the title ~~out-of-bounds write in libraw\src\x3f\x3f_utils_patched.cpp~~ **Libraw "new_node()" Out-of-bounds Write Vulnerability** on Jun 15, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants