New issue

Jump to bottom

Libraw "LibRaw::parseSonySRF()" Out-of-bounds Read Vulnerability #283

Closed **0xfoxone** opened this issue on May 10, 2020 · 1 comment

0xfoxone commented on May 10, 2020

Description:

There is an out-of-bounds read vulnerability within the "LibRaw::parseSonySRF()" function (libraw\src\metadata\sony.cpp) when processing srf files.

Steps to Reproduce:

poc (password: 0xfoxone):
https://drive.google.com/open?id=1r0wig5pSGUFhP3mDycIUcKMvnHamYaGJ

cmd:
magick.exe convert poc.srf new.bmp

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-7.0.10-7\VisualMagick\bin\magick.exe convert c:\poc.srf c:\new.bmp
Symbol search path is: srv*
Executable search path is:
ModLoad: 00007ff7 79300000 00007ff7 79312000 magick.exe
ModLoad: 00007ffd b0d20000 00007ffd b0f10000 ntdll.dll
ModLoad: 00007ffd 99d60000 00007ffd 99dd1000 C:\WINDOWS\System32\verifier.dll
Page heap: pid 0x1ED0: page heap enabled with flags 0x3.
ModLoad: 00007ffd af870000 00007ffd af922000 C:\WINDOWS\System32\KERNEL32.DLL
ModLoad: 00007ffd add60000 00007ffd ae004000 C:\WINDOWS\System32\KERNELBASE.dll
ModLoad: 00007ffd 87cf0000 00007ffd 87fe1000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_MagickCore_.dll
ModLoad: 00007ffd 886a0000 00007ffd 8886b000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_MagickWand_.dll
ModLoad: 00007ffd b01a0000 00007ffd b0334000 C:\WINDOWS\System32\USER32.dll
ModLoad: 00007ffd aea40000 00007ffd aea61000 C:\WINDOWS\System32\win32u.dll
ModLoad: 00007ffd af270000 00007ffd af296000 C:\WINDOWS\System32\GDI32.dll
ModLoad: 00007ffd ae010000 00007ffd ae1a4000 C:\WINDOWS\System32\gdi32full.dll
ModLoad: 00007ffd aea70000 00007ffd aeb0e000 C:\WINDOWS\System32\msvcp_win.dll
ModLoad: 00007ffd aeb30000 00007ffd aec2a000 C:\WINDOWS\System32\ucrtbase.dll
ModLoad: 00007ffd b04c0000 00007ffd b0563000 C:\WINDOWS\System32\ADVAPI32.dll
ModLoad: 00007ffd afdf0000 00007ffd afe8e000 C:\WINDOWS\System32\msvcrt.dll
ModLoad: 00007ffd b0420000 00007ffd b04b7000 C:\WINDOWS\System32\sechost.dll
ModLoad: 00007ffd af5b0000 00007ffd af6d0000 C:\WINDOWS\System32\RPCRT4.dll
ModLoad: 00007ffd afd80000 00007ffd afdef000 C:\WINDOWS\System32\WS2_32.dll
ModLoad: 00007ffd a1d20000 00007ffd a1d42000 C:\WINDOWS\SYSTEM32\VCRUNTIME140D.dll
ModLoad: 00007ffd 86800000 00007ffd 869bb000 C:\WINDOWS\SYSTEM32\ucrtbased.dll
ModLoad: 00007ffd 8d900000 00007ffd 8da1f000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_freetype_.dll
ModLoad: 00007ffd 8e600000 00007ffd 8e686000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_lcms_.dll
ModLoad: 00007ffd a1b50000 00007ffd a1b77000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_bzlib_.dll
ModLoad: 00007ffd 8e1c0000 00007ffd 8e260000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_libxml_.dll
ModLoad: 00007ffd 9dbe0000 00007ffd 9dc03000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_lqr_.dll
ModLoad: 00007ffd 9d610000 00007ffd 9d63a000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_zlib_.dll
ModLoad: 00007ffd 9a400000 00007ffd 9a435000 C:\WINDOWS\SYSTEM32\VCOMP140D.DLL
ModLoad: 00007ffd 85150000 00007ffd 8548b000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_glib_.dll
ModLoad: 00007ffd b05f0000 00007ffd b0cd4000 C:\WINDOWS\System32\SHELL32.dll
ModLoad: 00007ffd aed80000 00007ffd aedca000 C:\WINDOWS\System32\cfgmgr32.dll
ModLoad: 00007ffd afc70000 00007ffd afd19000 C:\WINDOWS\System32\shcore.dll
ModLoad: 00007ffd af930000 00007ffd afc66000 C:\WINDOWS\System32\combase.dll
ModLoad: 00007ffd ae1b0000 00007ffd ae230000 C:\WINDOWS\System32\bcryptPrimitives.dll
ModLoad: 00007ffd ae260000 00007ffd ae9dd000 C:\WINDOWS\System32\windows.storage.dll
ModLoad: 00007ffd adc80000 00007ffd adca3000 C:\WINDOWS\System32\profapi.dll
ModLoad: 00007ffd adbf0000 00007ffd adc3a000 C:\WINDOWS\System32\powrprof.dll
ModLoad: 00007ffd adbe0000 00007ffd adbf0000 C:\WINDOWS\System32\UMPDC.dll
ModLoad: 00007ffd b03c0000 00007ffd b0412000 C:\WINDOWS\System32\shlwapi.dll
ModLoad: 00007ffd adc40000 00007ffd adc51000 C:\WINDOWS\System32\kernel.appcore.dll
ModLoad: 00007ffd aeb10000 00007ffd aeb27000 C:\WINDOWS\System32\cryptsp.dll
ModLoad: 00007ffd b0040000 00007ffd b0197000 C:\WINDOWS\System32\ole32.dll
ModLoad: 00007ffd ad1b0000 00007ffd ad27b000 C:\WINDOWS\SYSTEM32\DNSAPI.dll
ModLoad: 00007ffd af370000 00007ffd af378000 C:\WINDOWS\System32\NSI.dll
ModLoad: 00007ffd ad160000 00007ffd ad19a000 C:\WINDOWS\SYSTEM32\IPHLPAPI.DLL
(1ed0.1214): Break instruction exception - code 80000003 (first chance)
ntdll!LdrpDoDebuggerBreak+0x30:
00007ffd b0df119c cc int 3 0:000> g ModLoad: 00007ffd af4b0000 00007ffd af4de000 C:\WINDOWS\System32\IMM32.DLL ModLoad: 00007ffd a93a0000 00007ffd a93af000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\IM_MOD_DB_DNG_.dll ModLoad: 00007ffd 86310000 00007ffd 864bc000 C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_libraw_.dll ModLoad: 00007ffd 88e10000 00007ffd 88f06000 C:\WINDOWS\SYSTEM32\MSVCP140D.dll (1ed0.1214): 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-7.0.10-7\VisualMagick\bin\CORE_DB_libraw_.dll CORE_DB_libraw_!LibRaw::sget2+0x2c: 00007ffd 86396d9c 0fb60401 movzx eax,byte ptr [rcx+rax] ds:0000019e 5bb50000=?? 0:000> k Child-SP RetAddr Call Site 00 00000093 9ecee890 00007ffd 8636bf5d CORE_DB_libraw_!LibRaw::sget2+0x2c [c:\imagemagick-7.0.10-7\libraw\src\utils\utils_dcraw.cpp @ 84] 01 00000093 9ecee8a0 00007ffd 8636fe7a CORE_DB_libraw_!LibRaw::parseSonySRF+0x42d [c:\imagemagick-7.0.10-7\libraw\src\metadata\sony.cpp @ 1952] 02 00000093 9ecee950 00007ffd 8638071a CORE_DB_libraw_!LibRaw::parse_exif+0x155a [c:\imagemagick-7.0.10-7\libraw\src\metadata\exif_gps.cpp @ 229] 03 00000093 9eceef50 00007ffd 8637bebb CORE_DB_libraw_!LibRaw::parse_tiff_ifd+0x484a [c:\imagemagick-7.0.10-7\libraw\src\metadata\tiff.cpp @ 717] 04 00000093 9ecefdd0 00007ffd 8632f89f CORE_DB_libraw_!LibRaw::parse_tiff+0x11b [c:\imagemagick-7.0.10-7\libraw\src\metadata\tiff.cpp @ 1468] 05 00000093 9ecefe30 00007ffd 864079de CORE_DB_libraw_!LibRaw::identify+0xd2f [c:\imagemagick-7.0.10-7\libraw\src\metadata\identify.cpp @ 537] 06 00000093 9ecf3350 00007ffd 8640b149 CORE_DB_libraw_!LibRaw::open_datastream+0x10e [c:\imagemagick-7.0.10-7\libraw\src\utils\open.cpp @ 377] 07 00000093 9ecf35f0 00007ffd 8641dfc8 CORE_DB_libraw_!LibRaw::open_file+0x269 [c:\imagemagick-7.0.10-7\libraw\src\utils\open.cpp @ 99] *** WARNING: Unable to verify checksum for C:\ImageMagick-7.0.10-7\VisualMagick\bin\IM_MOD_DB_DNG_.dll 08 00000093 9ecf3720 00007ffd a93a191c CORE_DB_libraw_!libraw_open_wfile+0x58 [c:\imagemagick-7.0.10-7\libraw\src\libraw_c_api.cpp @ 113] *** WARNING: Unable to verify checksum for C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_MagickCore_.dll 09 00000093 9ecf3760 00007ffd 87d671e7 IM_MOD_DB_DNG_!ReadDNGImage+0x2fc [c:\imagemagick-7.0.10-7\imagemagick\coders\dng.c @ 379] 0a 00000093 9ecf5870 00007ffd 87d68963 CORE_DB_MagickCore_!ReadImage+0x5e7 [c:\imagemagick-7.0.10-7\imagemagick\magickcore\constitute.c @ 553] *** WARNING: Unable to verify checksum for C:\ImageMagick-7.0.10-7\VisualMagick\bin\CORE_DB_MagickWand_.dll 0b 00000093 9ecfaa90 00007ffd 886daac3 CORE_DB_MagickCore_!ReadImages+0x393 [c:\imagemagick-7.0.10-7\imagemagick\magickcore\constitute.c @ 941] 0c 00000093 9ecfbb40 00007ffd 887744ae CORE_DB_MagickWand_!ConvertImageCommand+0x1523 [c:\imagemagick-7.0.10-7\imagemagick\magickwand\convert.c @ 606] *** WARNING: Unable to verify checksum for magick.exe 0d 00000093 9ecfd690 00007ff7 793014ea CORE_DB_MagickWand_!MagickCommandGenesis+0x33e [c:\imagemagick-7.0.10-7\imagemagick\magickwand\mogrify.c @ 186] 0e 00000093 9ecfe800 00007ff7 79301693 magick!MagickMain+0x4ea [c:\imagemagick-7.0.10-7\imagemagick\utilities\magick.c @ 149] 0f 00000093 9ecffa70 00007ff7 79301f24 magick!wmain+0x43 [c:\imagemagick-7.0.10-7\imagemagick\utilities\magick.c @ 195] 10 00000093 9ecffab0 00007ff7 79301e37 magick!invoke_main+0x34 [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 80] 11 00000093 9ecffaf0 00007ff7 79301cfe magick!__scrt_common_main_seh+0x127 [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 253] 12 00000093 9ecffb50 00007ff7 79301f39 magick!__scrt_common_main+0xe [f:\dd\vctools\crt\vcstartup\src\startup\exe_common.inl @ 296] 13 00000093 9ecffb80 00007ffd af887bd4 magick!wmainCRTStartup+0x9 [f:\dd\vctools\crt\vcstartup\src\startup\exe_wmain.cpp @ 17] 14 00000093 9ecffbb0 00007ffd b0d8ce51 KERNEL32!BaseThreadInitThunk+0x14 15 00000093 9ecffbe0 00000000`00000000 ntdll!RtlUserThreadStart+0x21

System Configuration:

- ImageMagick:
  Version: ImageMagick-7.0.10-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 May 10, 2020 Owner

Although not reproduced, this patch should improve things: `c243f45`

LibRaw closed this as completed on May 10, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants