New issue

Jump to bottom

ImageMagick "ReadHEICImageByID()" Out-of-bounds read vulnerability #1859

Closed GirlElecta opened this issue on Mar 3, 2020 · 6 comments

Labels bug

GirlElecta commented on Mar 3, 2020 • edited

Prerequisites

- [Y] I have written a descriptive issue title
- [Y] I have verified that I am using the latest version of ImageMagick
- [Y] I have searched open and closed issues to ensure it has not already been reported

Description

An out-of-bounds read vulnerability exists within the "ReadHEICImageByID()" function (ImageMagick\coders\heic.c) which can be triggered via an image with width or height in pixel more than length or actual physical size of the image.

Steps to Reproduce

(poc archive password= girlelecta):
https://drive.google.com/file/d/1N5gcCo7C9yhBGgnBM4AMMngwq95x3uXn/view

cmd:
magick.exe convert poc.heic new.png

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

Microsoft (R) Windows Debugger Version 10.0.17763.132 X86
Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: C:\Program Files\ImageMagick-7.0.9-Q16\magick.exe convert C:\Users\test\Desktop\poc.heic c:\a.png

```
************* Path validation summary **************
Response Time (ms) Location
Executable search path is:
ModLoad: 000f0000 000fb000 image000f0000
ModLoad: 77e00000 77f99000 ntdll.dll
ModLoad: 60ee0000 60f43000 C:\WINDOWS\System32\verifier.dll
Page heap: pid 0xD04: page heap enabled with flags 0x3.
ModLoad: 77440000 774d8000 C:\WINDOWS\System32\KERNEL32.DLL
ModLoad: 756f0000 758ea000 C:\WINDOWS\System32\KERNELBASE.dll
ModLoad: 7b680000 7b76e000 C:\Program Files\ImageMagick-7.0.9-Q16\MSVCR120.dll
ModLoad: 797c0000 7994b000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_MagickCore_.dll
ModLoad: 7b5b0000 7b679000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_MagickWand_.dll
ModLoad: 6b620000 6b63d000 C:\Program Files\ImageMagick-7.0.9-Q16\VCOMP120.DLL
ModLoad: 764c0000 76638000 C:\WINDOWS\System32\USER32.dll
ModLoad: 75bd0000 75bec000 C:\WINDOWS\System32\win32u.dll
ModLoad: 77210000 77231000 C:\WINDOWS\System32\GDI32.dll
ModLoad: 75bf0000 75d4d000 C:\WINDOWS\System32\gdi32full.dll
ModLoad: 76320000 7639c000 C:\WINDOWS\System32\msvcp_win.dll
ModLoad: 75ab0000 75bcf000 C:\WINDOWS\System32\ucrtbase.dll
ModLoad: 77d80000 77df9000 C:\WINDOWS\System32\ADVAPI32.dll
ModLoad: 774e0000 7759f000 C:\WINDOWS\System32\msvcrt.dll
ModLoad: 766a0000 76716000 C:\WINDOWS\System32\sechost.dll
ModLoad: 76e10000 76ed1000 C:\WINDOWS\System32\RPCRT4.dll
ModLoad: 77620000 7767e000 C:\WINDOWS\System32\WS2_32.dll
ModLoad: 602c0000 60342000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_freetype_.dll
ModLoad: 68750000 68761000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_bzlib_.dll
ModLoad: 67a50000 67a94000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_lcms_.dll
ModLoad: 63f90000 63fe3000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_libxml_.dll
ModLoad: 70ca0000 70caf000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_lqr_.dll
ModLoad: 68410000 68425000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_zlib_.dll
ModLoad: 01530000 01545000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_zlib_.dll
ModLoad: 7c720000 7c90a000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_glib_.dll
ModLoad: 77800000 77d7a000 C:\WINDOWS\System32\SHELL32.dll
ModLoad: 759c0000 759fb000 C:\WINDOWS\System32\cfgmgr32.dll
ModLoad: 76d80000 76e04000 C:\WINDOWS\System32\shcore.dll
ModLoad: 76ee0000 77156000 C:\WINDOWS\System32\combase.dll
ModLoad: 758f0000 7594f000 C:\WINDOWS\System32\bcryptPrimitives.dll
ModLoad: 75d50000 76315000 C:\WINDOWS\System32\windows.storage.dll
ModLoad: 756d0000 756e7000 C:\WINDOWS\System32\profapi.dll
ModLoad: 75680000 756c3000 C:\WINDOWS\System32\powrprof.dll
ModLoad: 75650000 7565d000 C:\WINDOWS\System32\UMPDC.dll
ModLoad: 773f0000 77434000 C:\WINDOWS\System32\shlwapi.dll
ModLoad: 75660000 7566f000 C:\WINDOWS\System32\kernel.appcore.dll
ModLoad: 759a0000 759b3000 C:\WINDOWS\System32\cryptsp.dll
ModLoad: 77240000 77337000 C:\WINDOWS\System32\ole32.dll
ModLoad: 74d40000 74d72000 C:\WINDOWS\SYSTEM32\IPHLPAPI.DLL
ModLoad: 74d80000 74e11000 C:\WINDOWS\SYSTEM32\DNSAPI.dll
ModLoad: 767b0000 767b7000 C:\WINDOWS\System32\NSI.dll
ModLoad: 76780000 767a6000 C:\WINDOWS\System32\IMM32.DLL
ModLoad: 70b50000 70b57000 C:\Program Files\ImageMagick-7.0.9-Q16\modules\coders\IM_MOD_RL_HEIC_.dll
ModLoad: 60220000 60273000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_libheif_.dll
ModLoad: 51f90000 52001000 C:\Program Files\ImageMagick-7.0.9-Q16\MSVCP120.dll
ModLoad: 5b7e0000 5b840000 C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_libde265_.dll
(d04.1660): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Program Files\ImageMagick-7.0.9-Q16\modules\coders\IM_MOD_RL_HEIC_.dll -
eax=058341f0 ebx=00000356 ecx=0010ae10 edx=0000c0c0 esi=04a86c20 edi=00000010
eip=70b5199d esp=001f6390 ebp=076e2220 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010202
IM_MOD_RL_HEIC_+0x199d:
70b5199d 0fb60c01 movzx ecx,byte ptr [ecx+eax] ds:0023:0593f000=??
0:000> k
ChildEBP RetAddr
WARNING: Stack unwind information not available. Following frames may be wrong.
00 001f63dc 70b514e1 IM_MOD_RL_HEIC_+0x199d
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Program Files\ImageMagick-7.0.9-Q16\CORE_RL_MagickCore_.dll -
01 001f6430 797f7b05 IM_MOD_RL_HEIC_+0x14e1
02 001f644c 7985935f CORE_RL_MagickCore_!ReadImage+0x505
03 001f6454 798dbfa2 CORE_RL_MagickCore_!RelinquishMagickMemory+0xf
04 001f646c 798dc3be CORE_RL_MagickCore_!GetPathAttributes+0x52
05 001f64b8 798d530e CORE_RL_MagickCore_!IsPathAccessible+0x4e
06 001f64c8 798db98d CORE_RL_MagickCore_!GlobExpression+0x88e
07 001f64cc 798dbaa4 CORE_RL_MagickCore_!ExpandFilenames+0x22d
08 001f64dc 798dbb43 CORE_RL_MagickCore_!ExpandFilenames+0x344
09 001f6524 77e4207b CORE_RL_MagickCore_!ExpandFilenames+0x3e3
0a 001f65c0 77e41976 ntdll!RtlpAllocateHeapInternal+0x6db
*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Program Files\ImageMagick-7.0.9-Q16\MSVCR120.dll -
0b 001f65e0 7b68ed63 ntdll!RtlAllocateHeap+0x36
0c 00000000 00000000 MSVCR120!malloc+0x33
```

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

dlemstra added a commit that referenced this issue on Mar 3, 2020

`Always correct the width and height of the image (#1859).` 868aad7

dlemstra added the bug label on Mar 3, 2020

dlemstra commented on Mar 3, 2020 Member

It seems that we always need to call `heif_image_get_width` and `heif_image_get_height` after the image has been decoded. This will resolve the issue that you have reported. Thank you for reporting this. We have a patch to fix it in GIT master branch @ https://github.com/ImageMagick/ImageMagick later today. The patch will be available in the beta releases of ImageMagick @ https://www.imagemagick.org/download/beta/ by sometime tomorrow.

urban-warrior closed this as completed on Mar 7, 2020

nohmask commented on Mar 10, 2020

This was assigned CVE-2020-10251.

carnil commented on Mar 11, 2020 • edited

@dlemstra, although there is no `ReadHEICImageByID()` in ImageMagick6 is the issue specific to ImageMagick7? The POC seem to triggere invalid reads in `coders/heic` but this might be then another issue?

dlemstra commented on Mar 12, 2020 Member

This was also an issue in IM6. Resolved with the commit: ImageMagick/ImageMagick6@ `3456724`

fmw42 commented on Mar 12, 2020

Good. Thanks for catching that.

Fred
…

carnil commented on Mar 12, 2020

> On Wed, Mar 11, 2020 at 10:31:45PM -0700, Dirk Lemstra wrote:
> This was also an issue in IM6. Resolved with the commit: ImageMagick/ImageMagick6@ `3456724`

Thanks!

GirlElecta changed the title ~~out-of-bounds read in ImageMagick\coders\heic.c~~ **"ReadHEICImageByID()" Out-of-bounds read vulnerability** on Jun 15, 2020

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

Assignees

No one assigned

Labels

bug

Milestone

No milestone

Development

No branches or pull requests

6 participants