Bug 1891934 (CVE-2020-25676) - CVE-2020-25676 ImageMagick: outside the range of representable values of type 'long' and integer overflow at MagickCore/pixel.c and MagickCore/cache.c

Keywords:	Security ×	**Reported:**	2020-10-27 17:39 UTC by Guilherme de Almeida Suckevicz
Status:	CLOSED WONTFIX	**Modified:**	2021-02-11 19:19 UTC (History)
Alias:	CVE-2020-25676	**CC List:**	7 users (show)
Product:	Security Response	**Fixed In Version:**	ImageMagick 7.0.9-0
Component:	vulnerability	**Doc Type:**	If docs needed, set a value
Version:	unspecified	**Doc Text:**	A flaw was found ImageMagick. Multiple unconstrained pixel offset calculations produce undefined behavior in the form of out-of-range and integer overflows. These instances of undefined behavior could be triggered by an attacker who is able to supply a crafted input file. The highest threat from this vulnerability is to system availability.
Hardware:	All	**Clone Of:**	
OS:	Linux	**Environment:**	
Priority:	medium	**Last Closed:**	2020-11-24 23:34:14 UTC
Severity:	medium		
Target Milestone:	---		
Assignee:	Red Hat Product Security		
QA Contact:			
Docs Contact:			
URL:			
Whiteboard:			
Depends On:	~~1891239~~ ~~1891240~~ 1910558		
Blocks:	1891602		
TreeView+	depends on / blocked		

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Guilherme de Almeida Suckevicz 2020-10-27 17:39:18 UTC — Description

In ImageMagick 7.0.8-68 there are 2 outside the range of representable values of type 'long' and 5 integer overflow at MagickCore/pixel.c,cache.c.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1732

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/406da3af9e09649cda152663c179902edf5ab3ac

Todd Cullum 2020-10-28 22:53:22 UTC — Comment 1

Flaw summary:

In CatromWeights(), MeshInterpolate(), InterpolatePixelChannel(), InterpolatePixelChannels(), and InterpolatePixelInfo(), which are all functions in /MagickCore/pixel.c, there were multiple unconstrained pixel offset calculations which were being used with the floor() function. These calculations produced undefined behavior in the form of out-of-range and integer overflows, as identified by UndefinedBehaviorSanitizer.

These instances of undefined behavior could be triggered by an attacker who is able to supply a crafted input file to be processed by ImageMagick. These issues could impact application availability or potentially cause other problems related to undefined behavior.

Todd Cullum 2020-10-28 22:56:45 UTC — Comment 2

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-10-29 19:16:20 UTC — Comment 3

Statement:

This flaw is out of support scope for Red Hat Enterprise Linux 5, 6, and 7. Inkscape is not affected because it no longer uses a bundled ImageMagick in Red Hat Enterprise Linux 8. For more information regarding support scopes, please see https://access.redhat.com/support/policy/updates/errata .

Guilherme de Almeida Suckevicz 2020-11-24 19:07:07 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1891239~~]
Affects: fedora-all [~~bug 1891240~~]

Product Security DevOps Team 2020-11-24 23:34:14 UTC — Comment 5

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2020-25676

Note
You need to log in before you can comment on or make changes to this bug.