Bug 1894231 (CVE-2020-27754) - CVE-2020-27754 ImageMagick: outside the range of representable values of type 'long' and signed integer overflow at MagickCore/quantize.c

Keywords: Security ×

Status: CLOSED WONTFIX
Alias: CVE-2020-27754
Product: Security Response
Component: vulnerability
Version: unspecified
Hardware: All
OS: Linux
Priority: low
Severity: low
Target Milestone: ---
Assignee: Red Hat Product Security
QA Contact:
Docs Contact:
URL:
Whiteboard:
Depends On: ~~1901251~~ ~~1901252~~ 1910552
Blocks: 1891602
TreeView+ depends on / blocked

Reported: 2020-11-03 18:58 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-02-15 20:43 UTC (History)
CC List: 7 users (show)
Fixed In Version: ImageMagick 6.9.10-69, ImageMagick 7.0.8-69
Doc Type: If docs needed, set a value
Doc Text: In IntensityCompare() of /magick/quantize.c, there are calls to PixelPacketIntensity() which could return overflowed values to the caller when ImageMagick processes a crafted input file. To mitigate this, the patch introduces and uses the ConstrainPixelIntensity() function, which forces the pixel intensities to be within the proper bounds in the event of an overflow.
Clone Of:
Environment:
Last Closed: 2020-11-24 23:34:29 UTC

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

Guilherme de Almeida Suckevicz 2020-11-03 18:58:47 UTC — Description

In ImageMagick, there are outside the range of representable values of type 'long' and signed integer overflow at MagickCore/quantize.c.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1754

Upstream patch:
https://github.com/ImageMagick/ImageMagick6/commit/d5df600d43c8706df513a3273d09aee6f54a9233

Guilherme de Almeida Suckevicz 2020-11-03 18:58:50 UTC — Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-11-03 23:03:04 UTC — Comment 2

Flaw summary:

In IntensityCompare() of /magick/quantize.c, there are calls to PixelPacketIntensity() which could return overflowed values to the caller when ImageMagick processes a crafted input file. To mitigate this, the patch introduces and uses the ConstrainPixelIntensity() function, which forces the pixel intensities to be within the proper bounds in the event of an overflow.

Todd Cullum 2020-11-03 23:05:09 UTC — Comment 3

I marked this as impact Low because while the issue could potentially cause an impact to availability, none was demonstrated - UndefinedBehaviorSanitizer just showed that there is undefined behavior present.

Todd Cullum 2020-11-03 23:05:43 UTC — Comment 4

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 19:14:56 UTC — Comment 5

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901251~~]
Affects: fedora-all [~~bug 1901252~~]

Product Security DevOps Team 2020-11-24 23:34:29 UTC — Comment 6

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-2020-27754

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