Bug 1891612 (CVE-2020-25666) - CVE-2020-25666 ImageMagick: outside the range of representable values of type int and signed integer overflow in MagickCore/histogram.c

Keywords: Security ×

Status: CLOSED WONTFIX

Alias: CVE-2020-25666

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: ~~1901229~~ ~~1901230~~ 1910562

Blocks: 1891602

TreeView+ depends on / blocked

Reported: 2020-10-26 20:20 UTC by Guilherme de Almeida Suckevicz

Modified: 2021-02-15 20:42 UTC (History)

CC List: 7 users (show)

Fixed In Version: ImageMagick 7.0.9-0

Doc Type: If docs needed, set a value

Doc Text: There are 4 places in HistogramCompare() in MagickCore/histogram.c where an integer overflow is possible during simple math calculations. This occurs in the rgb values and `count` value for a color. The patch uses casts to `ssize_t` type for these calculations, instead of `int`. This flaw could impact application reliability in the event that ImageMagick processes a crafted input file.

Clone Of:

Environment:

Last Closed: 2020-11-24 23:34:01 UTC

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

Guilherme de Almeida Suckevicz 2020-10-26 20:20:12 UTC — Description

ImageMagick 7.0.8-68 there are 4 outside the range of representable values of type 'int' and a signed integer overflow at MagickCore/histogram.c.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1750

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/94691f00839dbdf43edb1508af945ab19b388573

Todd Cullum 2020-10-28 21:07:59 UTC — Comment 1

Flaw summary:

There are 4 places in HistogramCompare() in MagickCore/histogram.c where an integer overflow is possible during simple math calculations. This occurs in the rgb values and `count` value for a color. The patch uses casts to `ssize_t` type for these calculations, instead of `int`. This flaw could impact application reliability in the event that ImageMagick processes a crafted input file.

Todd Cullum 2020-10-28 21:09:39 UTC — Comment 2

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-10-29 19:12:08 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 19:01:16 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901229~~]
Affects: fedora-all [~~bug 1901230~~]

Product Security DevOps Team 2020-11-24 23:34:01 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-2020-25666

Note

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