Bug 1891933 (CVE-2020-25675) - CVE-2020-25675 ImageMagick: outside the range of representable values of type 'long' and integer overflow at MagickCore/transform.c and MagickCore/image.c

Keywords: Security ×

Status: CLOSED WONTFIX

Alias: CVE-2020-25675

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~1901236~~ ~~1901237~~ 🔒 1910559

Blocks: 🔒 1891602

TreeView+ depends on / blocked

Reported: 2020-10-27 17:34 UTC by Guilherme de Almeida Suckevicz

Modified: 2021-02-11 19:04 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: ❗ A flaw was found in ImageMagick. Rounding calculations performed on unconstrained pixel offsets causes undefined behavior in the form of integer overflow and out-of-range values. Such issues could cause a negative impact to application availability or other problems related to undefined behavior, in cases where ImageMagick processes untrusted input data. The highest threat from this vulnerability is to system availability.

Clone Of:

Environment:

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

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

Guilherme de Almeida Suckevicz 2020-10-27 17:34:53 UTC Description

In ImageMagick 7.0.8-68 there are 6 outside the range of representable values of type 'long' and 2 integer overflow at MagickCore/transform.c,image.c.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1731

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/64dc80b2e1907f7f20bf34d4df9483f938b0de71

Todd Cullum 2020-10-28 22:28:56 UTC Comment 1

Flaw summary:

In the CropImage() and CropImageToTiles() routines of MagickCore/transform.c, rounding calculations performed on unconstrained pixel offsets was causing undefined behavior in the form of integer overflow and out-of-range values as reported by UndefinedBehaviorSanitizer. Such issues could cause a negative impact to application availability or other problems related to undefined behavior, in cases where ImageMagick processes untrusted input data. The upstream patch introduces functionality to constrain the pixel offsets and prevent these issues.

Todd Cullum 2020-10-28 22:40:45 UTC Comment 2

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Guilherme de Almeida Suckevicz 2020-11-24 19:05:38 UTC Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901236~~]
Affects: fedora-all [~~bug 1901237~~]

Product Security DevOps Team 2020-11-24 23:34:11 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-2020-25675

~~Eric Christensen~~ 2021-02-11 19:04:20 UTC Comment 7

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.

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