Bug 1891928 (CVE-2020-25674) - CVE-2020-25674 ImageMagick: heap-based buffer overflow in WriteOnePNGImage in coders/png.c

Keywords: Security ×

Status: CLOSED WONTFIX

Alias: CVE-2020-25674

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: ~~1901233~~ ~~1901235~~ 🔒 1910560

Blocks: 🔒 1891602

TreeView+ depends on / blocked

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

Modified: 2021-02-11 18:43 UTC (History)

CC List: 7 users (show)

Fixed In Version: ImageMagick 7.0.8-68

Doc Type: ❗ If docs needed, set a value

Doc Text: ❗ A flaw was found in ImageMagick. When the colormap has less than 256 valid values, the loop condition will continue to loop 256 times, attempting to pass invalid colormap data to the event logger, leading to an improper exit condition and an out-of-bounds read via heap-buffer-overflow. The highest threat from this vulnerability is to system availability.

Clone Of:

Environment:

Last Closed: 2020-11-24 23:34:08 UTC

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

Guilherme de Almeida Suckevicz 2020-10-27 17:17:29 UTC — Description

In ImageMagick 7.0.8-67 there is a heap-buffer-overflow at coders/png.c:9026:46 in WriteOnePNGImage.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1715

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/67b871032183a29d3ca0553db6ce1ae80fddb9aa

Todd Cullum 2020-10-28 21:45:38 UTC — Comment 1

Flaw summary:

WriteOnePNGImage() from coders/png.c (the PNG coder) has a for loop with an improper exit condition that can allow an out-of-bounds READ via heap-buffer-overflow. This occurs because it is possible for the colormap to have less than 256 valid values but the loop condition will loop 256 times, attempting to pass invalid colormap data to the event logger. The patch replaces the hardcoded 256 value with a call to MagickMin() to ensure the proper value is used.

This could impact application availability when a specially crafted input file is processed by ImageMagick.

Todd Cullum 2020-10-28 21:49:20 UTC — Comment 2

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Guilherme de Almeida Suckevicz 2020-11-24 19:04:11 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901233~~]
Affects: fedora-all [~~bug 1901235~~]

Product Security DevOps Team 2020-11-24 23:34:08 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-2020-25674

~~Eric Christensen~~ 2021-02-11 18:43:24 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.