Bug 1891984 (CVE-2020-27750) - CVE-2020-27750 ImageMagick: division by zero in MagickCore/colorspace-private.h

Keywords:	Security ×
Status:	CLOSED WONTFIX
Alias:	CVE-2020-27750
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:	~~1901241~~ ~~1901242~~ 🔒 1910557
Blocks:	🔒 1891602
TreeView+	depends on / blocked

Reported:	2020-10-27 19:46 UTC by Guilherme de Almeida Suckevicz
Modified:	2021-02-16 19:00 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 in MagickCore/colorspace-private.h and MagickCore/quantum.h. This flaw allows an attacker who submits a crafted file that is processed by ImageMagick to trigger undefined behavior in the form of values outside the range of types `unsigned char` and math division by zero. The highest threat from this vulnerability is to system availability.
Clone Of:	
Environment:	
Last Closed:	2020-11-24 23:34:17 UTC

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

Guilherme de Almeida Suckevicz 2020-10-27 19:46:48 UTC Description

In ImageMagick 7.0.8-67 there are 3 division by zero at MagickCore/colorspace-private.h and outside the range bug at MagickCore/quantum.h:120.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1711

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/a81ca9a1b46a96be83682af3389f0a6f3d0d389d

Todd Cullum 2020-10-28 23:18:31 UTC Comment 1

Flaw Summary:

In ConvertRGBToCMYK() of MagickCore/colorspace-private.h , there are calculations involved in cyan, magenta, and yellow colors which could cause a divide-by-zero runtime error and crash ImageMagick when it is provided with untrusted input file data. The patch uses the function PerceptibleReciprocal() in addition to replacing division with multiplication, in order to avoid divide-by-zero conditions.

I'm not certain that the patch there fixes the out-of-range bug but that may have been patched elsewhere.

Todd Cullum 2020-10-28 23:21:27 UTC Comment 2

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-10-29 19:18:42 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 19:08:36 UTC Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901241~~]
Affects: fedora-all [~~bug 1901242~~]

Product Security DevOps Team 2020-11-24 23:34:17 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-2020-27750

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