Bug 1894233 (CVE-2020-27756) - CVE-2020-27756 ImageMagick: division by zero at MagickCore/geometry.c

Keywords: Security ×

Status: CLOSED WONTFIX
Alias: CVE-2020-27756
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: ~~1901257~~ ~~1901258~~ 1910550
Blocks: 1891602
TreeView+ depends on / blocked

Reported: 2020-11-03 19:12 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-02-15 19:24 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: In ParseMetaGeometry() of MagickCore/geometry.c, image height and width calculations can lead to divide-by-zero conditions which also lead to undefined behavior. This flaw can be triggered by a crafted input file processed by ImageMagick and could impact application availability. The patch uses multiplication in addition to the function `PerceptibleReciprocal()` in order to prevent such divide-by-zero conditions.
Clone Of:
Environment:
Last Closed: 2020-11-24 23:34:35 UTC

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

Guilherme de Almeida Suckevicz 2020-11-03 19:12:23 UTC — Description

In ImageMagick, a division by zero can lead to outside the range of representable value at MagickCore/geometry.c and signed integer overflow at MagickCore/decorate.c.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1725

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/f35eca82b0c294ff9d0ccad104a881c3ae2ba913

Guilherme de Almeida Suckevicz 2020-11-03 19:12:26 UTC — Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-11-03 23:54:49 UTC — Comment 2

Flaw summary:

In ParseMetaGeometry() of MagickCore/geometry.c, image height and width calculations can lead to divide-by-zero conditions which also lead to undefined behavior. This flaw can be triggered by a crafted input file processed by ImageMagick and could impact application availability. The patch uses multiplication in addition to the function `PerceptibleReciprocal()` in order to prevent such divide-by-zero conditions.

Todd Cullum 2020-11-03 23:56:14 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 19:18:54 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~Bug 1901257~~]
Affects: fedora-all [~~Bug 1901258~~]

Product Security DevOps Team 2020-11-24 23:34:35 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-2020-27756

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