Bug 1894236 (CVE-2020-27758) - CVE-2020-27758 ImageMagick: outside the range of representable values of type 'unsigned long long' at coders/txt.c

Keywords: Security ×

Status: CLOSED WONTFIX

Alias: CVE-2020-27758

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: ~~1901261~~ ~~1901262~~ 1910548

Blocks: 1891602

TreeView+ depends on / blocked

Reported: 2020-11-03 19:17 UTC by Guilherme de Almeida Suckevicz

Modified: 2021-02-15 20:46 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 coders/txt.c. An attacker who submits a crafted file that is processed by ImageMagick could trigger undefined behavior in the form of values outside the range of type `unsigned long long`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior.

Clone Of:

Environment:

Last Closed: 2020-11-24 23:34:41 UTC

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

Guilherme de Almeida Suckevicz 2020-11-03 19:17:35 UTC — Description

In ImageMagick, there are outside the range of representable values of type 'unsigned long long' bugs at coders/txt.c.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1719

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/f0a8d407b2801174fd8923941a9e7822f7f9a506

Guilherme de Almeida Suckevicz 2020-11-03 19:17:38 UTC — Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-11-04 20:19:50 UTC — Comment 2

In the txt coder at /coders/txt.c, ReadTXTImage() computes pixel values that could land outside the range of type unsigned long long due to improper max constraints. This flaw can be triggered when ImageMagick processes crafted input under certain conditions. Red Hat Product Security marked this as Low because although it could potentially lead to an impact to application availability, no specific impact was shown in this case.

Todd Cullum 2020-11-04 20:20:51 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 19:22:11 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901261~~]
Affects: fedora-all [~~bug 1901262~~]

Product Security DevOps Team 2020-11-24 23:34:41 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-2020-27758

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