Bug 1891994 (CVE-2020-27751) - CVE-2020-27751 ImageMagick: integer overflow in MagickCore/quantum-export.c

Keywords: Security ×

Status: CLOSED WONTFIX
Alias: CVE-2020-27751
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: ~~1901243~~ ~~1901244~~ 1910556
Blocks: 1891602
TreeView+ depends on / blocked

Reported: 2020-10-27 20:11 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-02-15 20:43 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 in MagickCore/quantum-export.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` as well as a shift exponent that is too large for 64-bit type. 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 23:34:20 UTC

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

Guilherme de Almeida Suckevicz 2020-10-27 20:11:53 UTC — Description

In ImageMagick 7.0.8-68 there are shift exponent 65 is too large for 64-bit type at MagickCore/quantum-export.c and outside the range of representable values of type 'unsigned long long' at MagickCore/quantum-private.h.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1727

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/f60d59cc3a7e3402d403361e0985ffa56f746a82

Todd Cullum 2020-10-29 17:40:41 UTC — Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-10-29 19:20:43 UTC — Comment 2

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 19:10:03 UTC — Comment 3

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901243~~]
Affects: fedora-all [~~bug 1901244~~]

Product Security DevOps Team 2020-11-24 23:34:20 UTC — Comment 4

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-2020-27751

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