Bug 1894234 (CVE-2020-27757) - CVE-2020-27757 ImageMagick: outside the range of representable values of type 'unsigned long long' at MagickCore/quantum-private.h

Keywords: Security ×

Status: CLOSED WONTFIX
Alias: CVE-2020-27757
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: ~~1901259~~ ~~1901260~~ 1910549
Blocks: 1891602
TreeView+ depends on / blocked

Reported: 2020-11-03 19:15 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-02-15 20:45 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 floating point math calculation in ScaleAnyToQuantum() of /MagickCore/quantum-private.h could lead to undefined behavior in the form of a value outside the range of type unsigned long long. The flaw could be triggered by a crafted input file under certain conditions when it is processed by ImageMagick.
Clone Of:
Environment:
Last Closed: 2020-11-24 23:34:38 UTC

Attachments (Terms of Use)

Add an attachment (proposed patch, testcase, etc.)

Guilherme de Almeida Suckevicz 2020-11-03 19:15:11 UTC — Description

In ImageMagick, there is an outside the range of representable values of type 'unsigned long long' bug at MagickCore/quantum-private.h.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1712

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/e88532bd4418e95b70cbc415fe911d22ab27a5fd

Guilherme de Almeida Suckevicz 2020-11-03 19:15:13 UTC — Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-11-04 20:08:54 UTC — Comment 2

Flaw summary:

A floating point math calculation in ScaleAnyToQuantum() of /MagickCore/quantum-private.h could lead to undefined behavior in the form of a value outside the range of type unsigned long long. The flaw could be triggered by a crafted input file under certain conditions when it is processed by ImageMagick. 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.

Guilherme de Almeida Suckevicz 2020-11-24 19:20:37 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~Bug 1901259~~]
Affects: fedora-all [~~Bug 1901260~~]

Product Security DevOps Team 2020-11-24 23:34:38 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-2020-27757

~~Eric Christensen~~ 2021-02-15 20:45:50 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.

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.

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