Bug 1894687 (CVE-2020-27767) - **CVE-2020-27767** ImageMagick: outside the range of representable values of type 'float' at MagickCore/quantum.h

Keywords:	Security ✕ ▼
Status:	CLOSED WONTFIX
Alias:	CVE-2020-27767
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:	~~1901270~~ ~~1901280~~ 🔒 1910538
Blocks:	🔒 1891602
TreeView+	depends on / blocked

Reported:	2020-11-04 19:11 UTC by Guilherme de Almeida Suckevicz
Modified:	2021-02-15 20:52 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.h. 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 types `float` and `unsigned char`. 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 23:35:08 UTC

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

Guilherme de Almeida Suckevicz   2020-11-04 19:11:05 UTC   Description

In ImageMagick, there are an outside the range of representable values of type 'float' at MagickCore/quantum.h:87 and outside the range of representable values of type 'unsigned char' at MagickCore/quantum.h.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1741

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/564f2a35e523e2b6cce9485018157f03ec05a947

Guilherme de Almeida Suckevicz   2020-11-04 19:11:07 UTC   Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum   2020-11-05 22:51:31 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 .

Todd Cullum   2020-11-05 22:52:16 UTC   Comment 3

Red Hat Product Security marked this as Low severity because although it could potentially lead to an impact to application availability, no specific impact was demonstrated in this case.

Guilherme de Almeida Suckevicz   2020-11-24 19:27:15 UTC   Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901270~~]
Affects: fedora-all [~~bug 1901280~~]

Product Security DevOps Team   2020-11-24 23:35:08 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-2020-27767

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