Bug 1898295 (CVE-2020-27773) - CVE-2020-27773 ImageMagick: division by zero at MagickCore/gem-private.h

Keywords:	Security ×	**Reported:**	2020-11-16 18:36 UTC by Guilherme de Almeida Suckevicz
Status:	CLOSED WONTFIX	**Modified:**	2021-02-15 20:56 UTC (History)
Alias:	CVE-2020-27773	**CC List:**	7 users (show)
Product:	Security Response	**Fixed In Version:**	ImageMagick 7.0.9-0
Component:	vulnerability	**Doc Type:**	If docs needed, set a value
Version:	unspecified	**Doc Text:**	A flaw was found in ImageMagick in MagickCore/gem-private.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 type `unsigned char` or division by zero. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior.
Hardware:	All	**Clone Of:**	
OS:	Linux	**Environment:**	
Priority:	low	**Last Closed:**	2020-11-24 23:35:26 UTC
Severity:	low		
Target Milestone:	---		
Assignee:	Red Hat Product Security		
QA Contact:			
Docs Contact:			
URL:			
Whiteboard:			
Depends On:	~~1901201~~ ~~1901202~~ 1910529		
Blocks:	1891602		

TreeView+ depends on / blocked

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

Guilherme de Almeida Suckevicz 2020-11-16 18:36:59 UTC — Description

In ImageMagick, there is a division by zero at MagickCore/gem-private.h and an outside the range of representable values of type 'unsigned char' at MagickCore/quantum.h.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1739

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/3d71aa8265ffaaf686021a6fbd54c037f71ee3a2

Guilherme de Almeida Suckevicz 2020-11-16 18:37:02 UTC — Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-11-16 20:56:49 UTC — Comment 2

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.

Todd Cullum 2020-11-16 20:57:53 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 19:30:10 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901201~~]
Affects: fedora-all [~~bug 1901202~~]

Product Security DevOps Team 2020-11-24 23:35:26 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-2020-27773

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