Bug 1898291 (CVE-2020-27772) - **CVE-2020-27772** ImageMagick: outside the range of representable values of type 'unsigned int' at coders/bmp.c

Keywords:	Security ✕ ▾	**Reported:**	2020-11-16 18:33 UTC by Guilherme de Almeida Suckevicz
		Modified:	2021-02-15 20:55 UTC (History)
Status:	CLOSED WONTFIX	**CC List:**	7 users (show)
Alias:	CVE-2020-27772		
Product:	Security Response	**Fixed In Version:**	ImageMagick 7.0.9-0
Component:	vulnerability	**Doc Type:**	❶ If docs needed, set a value
Version:	unspecified	**Doc Text:**	❶ A flaw was found in ImageMagick in coders/bmp.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 int`. This would most likely lead to an impact to application availability, but could potentially cause other problems related to undefined behavior.
Hardware:	All		
OS:	Linux		
Priority:	low	**Clone Of:**	
Severity:	low	**Environment:**	
Target Milestone:	---	**Last Closed:**	2020-11-24 23:35:24 UTC
Assignee:	Red Hat Product Security		
QA Contact:			
Docs Contact:			
URL:			
Whiteboard:			
Depends On:	1901280 1901200 🔒 1910530		
Blocks:	🔒 1891602		
TreeView+	depends on / blocked		

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

Guilherme de Almeida Suckevicz   2020-11-16 18:33:17 UTC   *Description*

In ImageMagick, there are 9 outside the range of representable values of type 'unsigned int' at coders/bmp.c.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1749

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/a1142af44f61c038ad3eccc099c5b9548b507846

Guilherme de Almeida Suckevicz   2020-11-16 18:33:19 UTC   *Comment 1*

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum   2020-11-16 20:26:33 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   2020-11-16 20:30:20 UTC   *Comment 3*

Flaw Summary:

There are numerous rgb & gamma calculations in WriteBMPImage() from /coders/bmp.c that can lead to undefined behavior in the form of values outside of the range of unsigned int. The patch addresses 12 areas by casting to ssize_t. These can be triggered when ImageMagick processes a crafted input file. 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 19:29:43 UTC   *Comment 4*

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [bug 1901209]
Affects: fedora-all [bug 1901210]

Product Security DevOps Team   2020-11-24 23:35:24 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-2020-27772