

Bug 1894686 (CVE-2020-27766) - CVE-2020-27766 ImageMagick: outside the range of representable values of type 'unsigned long' at MagickCore/statistic.c

Keywords: Security ×

Status: CLOSED WONTFIX

Alias: CVE-2020-27766

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: 4004377 4004378 🛡️ 1910539

Blocks: 🛡️ 1891602

TreeView+ depends on / blocked

Reported: 2020-11-04 19:08 UTC by Guilherme de Almeida Suckevicz

Modified: 2022-04-26 14:37 UTC (History)

CC List: 7 users (show)

Fixed In Version: ImageMagick 7.0.8-69

Doc Type: 🚩 If docs needed, set a value

Doc Text: 🚩 A flaw was found in ImageMagick in MagickCore/statistic.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'. 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 23:35:05 UTC

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

Guilherme de Almeida Suckevicz	2020-11-04 19:08:52 UTC	Description
In ImageMagick, there is an outside the range of representable values of type 'unsigned long' at MagickCore/statistic.c. Reference: https://github.com/ImageMagick/ImageMagick/issues/1734		
Guilherme de Almeida Suckevicz	2020-11-04 19:08:54 UTC	Comment 1
Acknowledgments: Name: Suhwan Song (Seoul National University)		
Todd Cullum	2020-11-04 22:42:52 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	2020-11-04 22:43:56 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 shown in this case.		
Guilherme de Almeida Suckevicz	2020-11-24 19:26:34 UTC	Comment 4
Created ImageMagick tracking bugs for this issue: Affects: epel-8 [bug-1901277] Affects: fedora-all [bug-1901278]		
Product Security DevOps Team	2020-11-24 23:35:05 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-2020-27766		

Note

You need to [log in](#) before you can comment on or make changes to this bug.