Bug 1894691 (CVE-2020-27770) - CVE-2020-27770 ImageMagick: unsigned offset overflowed at MagickCore/string.c

Keywords: Security ×

Status: CLOSED WONTFIX
Alias: CVE-2020-27770
Product: Security Response
Component: vulnerability
Version: unspecified
Hardware: All
OS: Linux
Priority: medium
Severity: medium
Target Milestone: ---
Assignee: Red Hat Product Security
QA Contact:
Docs Contact:
URL:
Whiteboard:
Depends On: ~~1901285~~ ~~1901286~~ 🔒 1910534
Blocks: 🔒 1891602
TreeView+ depends on / blocked

Reported: 2020-11-04 19:21 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-02-15 20:41 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: Due to a missing check for 0 value of `replace_extent`, it is possible for offset `p` to overflow in SubstituteString(), causing potential impact to application availability. This could be triggered by a crafted input file that is processed by ImageMagick.
Clone Of:
Environment:
Last Closed: 2020-11-24 23:35:18 UTC

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

Guilherme de Almeida Suckevicz 2020-11-04 19:21:56 UTC — Description

In ImageMagick, there is an integer overflow in MagickCore/string.c.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1721

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/be90a5395695f0d19479a5d46b06c678be7f7927

Guilherme de Almeida Suckevicz 2020-11-04 19:21:58 UTC — Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-11-05 23:06:54 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 23:12:33 UTC — Comment 3

Flaw summary:

Due to a missing check for 0 value of `replace_extent`, it is possible for offset `p` to overflow in SubstituteString(), causing potential impact to application availability. This could be triggered by a crafted input file that is processed by ImageMagick.

Guilherme de Almeida Suckevicz 2020-11-24 19:28:48 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901285~~]
Affects: fedora-all [~~bug 1901286~~]

Product Security DevOps Team 2020-11-24 23:35:18 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-2020-27770

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