Bug 1898290 (CVE-2020-27771) - CVE-2020-27771 ImageMagick: outside the range of representable values of type 'unsigned char' at coders/pdf.c

Keywords: Security ×

Status: CLOSED WONTFIX
Alias: CVE-2020-27771
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: ~~1901287~~ ~~1901288~~ 1910532
Blocks: 1891602
TreeView+ depends on / blocked

Reported: 2020-11-16 18:30 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-02-15 20:55 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: In RestoreMSCWarning() of /coders/pdf.c there are several areas where calls to GetPixelIndex() could result in values outside the range of representable for the unsigned char type. The patch casts the return value of GetPixelIndex() to ssize_t type to avoid this bug. This undefined behavior could be triggered when ImageMagick processes a crafted pdf file.
Clone Of:
Environment:
Last Closed: 2020-11-24 23:35:21 UTC

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

Guilherme de Almeida Suckevicz 2020-11-16 18:30:56 UTC — Description

In ImageMagick, there is an outside the range of representable values of type 'unsigned char' at coders/pdf.c.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1753

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/872ffe6d0131beec8b47568a4874ffaca91a872e
https://github.com/ImageMagick/ImageMagick/commit/9dd1c7e1f8f6c137bfd3293be2554f59456c7b62

Guilherme de Almeida Suckevicz 2020-11-16 18:30:59 UTC — Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-11-16 20:15:44 UTC — Comment 3

Flaw summary:

In RestoreMSCWarning() of /coders/pdf.c there are several areas where calls to GetPixelIndex() could result in values outside the range of representable for the unsigned char type. The patch casts the return value of GetPixelIndex() to ssize_t type to avoid this bug. This undefined behavior could be triggered when ImageMagick processes a crafted pdf 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 19:29:15 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901287~~]
Affects: fedora-all [~~bug 1901288~~]

Product Security DevOps Team 2020-11-24 23:35:21 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-2020-27771

~~Eric Christensen~~ 2021-02-15 20:55:13 UTC — Comment 7

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 .

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.

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