Bug 1891613 (CVE-2020-25667) - CVE-2020-25667 ImageMagick: heap-based buffer overflow in TIFFGetProfiles in coders/tiff.c

Keywords: Security ×

Status: CLOSED WONTFIX
Alias: CVE-2020-25667
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: ~~1901231~~ ~~1901232~~ 1910561
Blocks: 1891602
TreeView+ depends on / blocked

Reported: 2020-10-26 20:28 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-02-09 18:22 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: A flaw was found in TIFFGetProfiles() in /coders/tiff.c calls strstr(), which causes a large out-of-bounds read when it searches for `"dc:format=\"image/dng\"` within `profile` due to improper string handling when a crafted input file is provided to ImageMagick. The patch uses a StringInfo type instead of a raw C string to remedy this issue. The highest threat from this vulnerability is to system availability.
Clone Of:
Environment:
Last Closed: 2020-11-24 23:34:05 UTC

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

Guilherme de Almeida Suckevicz 2020-10-26 20:28:26 UTC — Description

ImageMagick 7.0.8-68 there is a heap-buffer-overflow at coders/tiff.c in TIFFGetProfiles.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1748

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/986b5dff173413fa712db27eb677cdef15f0bab6

Todd Cullum 2020-10-28 21:27:29 UTC — Comment 1

Flaw summary:

TIFFGetProfiles() in /coders/tiff.c calls strstr() which causes a large out-of-bounds read when it searches for `"dc:format=\"image/dng\"` within `profile` due to improper string handling, when a crafted input file is provided to ImageMagick. The patch uses a StringInfo type instead of a raw C string to remedy this. This could cause an impact to availability of the application.

Todd Cullum 2020-10-28 21:28:35 UTC — Comment 2

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-10-29 19:13:04 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 19:02:44 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901231~~]
Affects: fedora-all [~~bug 1901232~~]

Product Security DevOps Team 2020-11-24 23:34:05 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-2020-25667

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