Bug 1891606 (CVE-2020-25665) - CVE-2020-25665 ImageMagick: heap-based buffer overflow in WritePALMImage in coders/palm.c

Keywords: Security ×

Status: CLOSED WONTFIX
Alias: CVE-2020-25665
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: ~~1901227~~ ~~1901228~~ 1910564
Blocks: 1891602
TreeView+ depends on / blocked

Reported: 2020-10-26 19:59 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-04-05 14:55 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: A flaw was found in the PALM image coder at coders/palm.c where it makes an improper call to AcquireQuantumMemory() in the WritePALMImage() routine because it needs to be offset by 256. This issue causes an out-of-bounds read later on in the routine. The patch adds 256 to bytes_per_row in the call to AcquireQuantumMemory(). The highest threat from this vulnerability is to system availability.
Clone Of:
Environment:
Last Closed: 2020-11-24 23:33:59 UTC

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

Guilherme de Almeida Suckevicz 2020-10-26 19:59:07 UTC — Description

In ImageMagick, there is a heap-buffer-over-flow at coders/palm.c:956:21 in WritePALMImage.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1714

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/cfd829bd3581b092e0a267b3deba46fa90b9bc88

Todd Cullum 2020-10-28 20:57:00 UTC — Comment 1

Flaw summary:

The PALM image coder at coders/palm.c makes an improper call to AcquireQuantumMemory() in routine WritePALMImage() because it needs to be offset by 256. This can cause a out-of-bounds read later on in the routine. The patch adds 256 to bytes_per_row in the call to AcquireQuantumMemory(). This could cause impact to reliability.

Todd Cullum 2020-10-28 21:12:12 UTC — Comment 2

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-10-29 19:11:23 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 18:59:48 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901227~~]
Affects: fedora-all [~~bug 1901228~~]

Product Security DevOps Team 2020-11-24 23:33:59 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-2020-25665

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