Bug 1891605 (CVE-2020-25664) - CVE-2020-25664 ImageMagick: heap-based buffer overflow in PopShortPixel in MagickCore/quantum-private.h

Keywords: Security ×

Status: CLOSED WONTFIX
Alias: CVE-2020-25664
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: ~~1901225~~ ~~1901226~~ 🔒 1910565
Blocks: 🔒 1891602
TreeView+ depends on / blocked

Reported: 2020-10-26 19:48 UTC by Guilherme de Almeida Suckevicz
Modified: 2021-02-11 18:37 UTC (History)
CC List: 7 users (show)
Fixed In Version: ImageMagick 7.0.8-68, ImageMagick 6.9.10-68
Doc Type: If docs needed, set a value
Doc Text:

```
A flaw was found in ImageMagick. A specially
crafted image could cause an out-of-bounds memory
write leading to a crash. The highest threat from
this vulnerability is to system availability.
```

Clone Of:
Environment:
Last Closed: 2020-11-24 23:33:56 UTC

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

Guilherme de Almeida Suckevicz 2020-10-26 19:48:51 UTC Description

```
In ImageMagick, there is a heap-buffer-overflow at MagickCore/quantum-private.h:227:12 in PopShortPixel.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1716

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/1f450bb5ba53d275de6d1cd086c98a0b549ad393
```

Todd Cullum 2020-10-28 20:40:05 UTC Comment 1

```
Flaw summary:

In WriteOnePNGImage() of the PNG coder at coders/png.c, an improper call to AcquireVirtualMemory() and memset() allows for an out-of-bounds write later when
PopShortPixel() from MagickCore/quantum-private.h is called. The patch fixes the calls by adding 256 to rowbytes. An attacker who is able to supply a specially
crafted image could affect availability with a low impact to data integrity.
```

Todd Cullum 2020-10-28 21:13:09 UTC Comment 2

```
Acknowledgments:

Name: Suhwan Song (Seoul National University)
```

Todd Cullum 2020-10-29 19:10:26 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 18:57:40 UTC Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901225~~]
Affects: fedora-all [~~bug 1901226~~]

Product Security DevOps Team 2020-11-24 23:33:56 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-2020-25664
```

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