Bug 1894226 (CVE-2020-27752) - CVE-2020-27752 ImageMagick: heap-based buffer overflow in PopShortPixel in MagickCore/quantum-private.h

Keywords:	Security ×
Status:	CLOSED WONTFIX
Alias:	CVE-2020-27752
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:	~~1901247~~ ~~1901248~~ 1910554
Blocks:	1891602
TreeView+	depends on / blocked

Reported:	2020-11-03 18:40 UTC by Guilherme de Almeida Suckevicz
Modified:	2021-04-29 23:39 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 ImageMagick in MagickCore/quantum-private.h. This flaw allows an attacker who submits a crafted file processed by ImageMagick to trigger a heap buffer overflow. The highest threat from this vulnerability is to system availability and also a potential impact on data integrity.
Clone Of:	
Environment:	
Last Closed:	2020-11-24 23:34:23 UTC

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

Guilherme de Almeida Suckevicz 2020-11-03 18:40:42 UTC Description

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

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1752

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/a9d563d3d73874312080d30dc4ba07cecad56192
```

Guilherme de Almeida Suckevicz 2020-11-03 18:40:44 UTC Comment 1

```
Acknowledgments:

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

Todd Cullum 2020-11-03 22:37:44 UTC Comment 2

```
This looks like the fix for CVE-2020-25664 was an incomplete fix hence the second reproducer which triggers the same thing via the same code path after the patch
was applied.
```

Todd Cullum 2020-11-03 22:41:41 UTC Comment 4

```
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 19:11:55 UTC Comment 6

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901247~~]
Affects: fedora-all [~~bug 1901248~~]

Product Security DevOps Team 2020-11-24 23:34:23 UTC Comment 7

```
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-2020-27752
```

Note

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