Bug 1894229 (CVE-2020-27753) - CVE-2020-27753 ImageMagick: memory leaks in AcquireMagickMemory function

Keywords:	Security ×
Status:	CLOSED WONTFIX
Alias:	CVE-2020-27753
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:	~~1901249~~ ~~1901250~~ 1910553
Blocks:	1891602
TreeView+	depends on / blocked

Reported:	2020-11-03 18:53 UTC by Guilherme de Almeida Suckevicz
Modified:	2021-02-15 19:23 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:	There are several memory leaks in the MIFF coder in /coders/miff.c due to improper image depth values, which can be triggered by a specially crafted input file. These leaks could potentially lead to an impact to application availability or cause a denial of service. It was originally reported that the issues were in \`AcquireMagickMemory()\` because that is where LeakSanitizer detected the leaks, but the patch resolves issues in the MIFF coder, which incorrectly handles data being passed to \`AcquireMagickMemory()\`.
Clone Of:	
Environment:	
Last Closed:	2020-11-24 23:34:26 UTC

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

Guilherme de Almeida Suckevicz 2020-11-03 18:53:13 UTC — Description

In ImageMagick, there are memory leaks detected in AcquireMagickMemory.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1757

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/bb3acad195de95db86c7509d8072db01890470e0

Guilherme de Almeida Suckevicz 2020-11-03 18:53:16 UTC — Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-11-03 22:54:07 UTC — Comment 2

Flaw summary:

There are several memory leaks in the MIFF coder in /coders/miff.c due to improper image depth values, which can be triggered by a specially crafted input file. These leaks could potentially lead to an impact to application availability or cause a denial of service. It was originally reported that the issues were in \`AcquireMagickMemory()\` because that is where LeakSanitizer detected the leaks, but the patch resolves issues in the MIFF coder, which incorrectly handles data being passed to \`AcquireMagickMemory()\`.

Todd Cullum 2020-11-03 22:54:44 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 19:13:29 UTC — Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901249~~]
Affects: fedora-all [~~bug 1901250~~]

Product Security DevOps Team 2020-11-24 23:34:26 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-2020-27753

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