Bug 1894232 (CVE-2020-27755) - CVE-2020-27755 ImageMagick: memory leaks in ResizeMagickMemory function in ImageMagick/MagickCore/memory.c

Keywords: Security ×

Status: CLOSED WONTFIX

Alias: CVE-2020-27755

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~1901253~~ ~~1901254~~ 🔒 1910551

Blocks: 🔒 1891602

TreeView+ depends on / blocked

Reported: 2020-11-03 19:03 UTC by Guilherme de Almeida Suckevicz

Modified: 2021-02-15 20:44 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: in SetImageExtent() of /MagickCore/image.c, an incorrect image depth size can cause a memory leak because the code which checks for the proper image depth size does not reset the size in the event there is an invalid size. The patch resets the depth to a proper size before throwing an exception. The memory leak can be triggered by a crafted input file that is processed by ImageMagick and could cause an impact to application reliability, such as denial of service.

Clone Of:

Environment:

Last Closed: 2020-11-24 23:34:32 UTC

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

Guilherme de Almeida Suckevicz 2020-11-03 19:03:33 UTC Description

In ImageMagick, there are memory leaks detected in ResizeMagickMemory at MagickCore/memory.c.

Reference:
https://github.com/ImageMagick/ImageMagick/issues/1756

Upstream patch:
https://github.com/ImageMagick/ImageMagick/commit/f28e9e56e1b56d4e1f09d2a56d70892ae295d6a4

Guilherme de Almeida Suckevicz 2020-11-03 19:03:35 UTC Comment 1

Acknowledgments:

Name: Suhwan Song (Seoul National University)

Todd Cullum 2020-11-03 23:19:18 UTC Comment 2

Flaw summary:

in SetImageExtent() of /MagickCore/image.c, an incorrect image depth size can cause a memory leak because the code which checks for the proper image depth size does not reset the size in the event there is an invalid size. The patch resets the depth to a proper size before throwing an exception. The memory leak can be triggered by a crafted input file that is processed by ImageMagick and could cause an impact to application reliability, such as denial of service.

Todd Cullum 2020-11-03 23:21:21 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 19:17:10 UTC Comment 4

Created ImageMagick tracking bugs for this issue:

Affects: epel-8 [~~bug 1901253~~]
Affects: fedora-all [~~bug 1901254~~]

Product Security DevOps Team 2020-11-24 23:34:32 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-2020-27755

Note

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