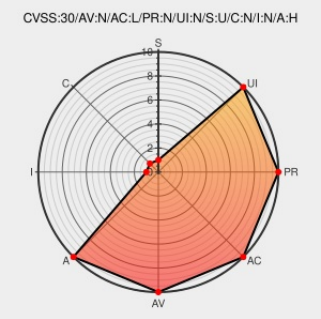
CVE-2017-14739

Published on: 09/25/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:44 PM UTC

CVE-2017-14739

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Imagemagick from Imagemagick contain the following vulnerability:

The AcquireResampleFilterThreadSet function in magick/resample-private.h in ImageMagick 7.0.7-4 mishandles failed memory allocation, which allows remote attackers to cause a denial of service (NULL Pointer Dereference in DistortImage in MagickCore/distort.c, and application crash) via unspecified vectors.

CVE-2017-14739 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 2366-1] imagemagick security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200907 [SECURITY] [DLA 2366-1] imagemagick security update

USN-3681-1: ImageMagick vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-3681-1
[SECURITY] [DLA 1785-1] imagemagick security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20190514 [SECURITY] [DLA 1785-1] imagemagick security update
Null Pointer Dereference at DistortImage of MagickCore/distort.c · Issue #780 · ImageMagick/ImageMagick · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM github.com/ImageMagick/ImageMagick/issues/780

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagemagick	Imagemagick	7.0.7-4	All	All	All
Application	Imagemagick	Imagemagick	7.0.7-4	All	All	All

cpe:2.3:a:imagemagick:imagemagick:7.0.7-4:*:*:*:*:*:*:*:

cpe:2.3:a:imagemagick:imagemagick:7.0.7-4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→