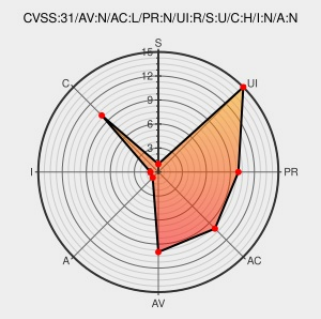
CVE-2017-11448

Published on: 07/19/2017 12:00:00 AM UTC

Last Modified on: 04/28/2021 05:51:00 PM UTC

CVE-2017-11448

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



Certain versions of Imagemagick from Imagemagick contain the following vulnerability:

The ReadJPEGImage function in coders/jpeg.c in ImageMagick before 7.0.6-1 allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted file.

CVE-2017-11448 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Zero pixel buffer · ImageMagick/ImageMagick@f6463ca · GitHub	Patch, Vendor Advisory, github.com, text/html	CONFIRM github.com/I

Comment about commit https://github.com/ImageMagick/ImageMagick/commit/1737ac82b335e53376382c07b9a500d73dd2aa11 · Issue #556 · ImageMagick/ImageMagick · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	CONFIRM
#867893 - imagemagick: CVE-2017-11448 - Debian Bug report logs	Issue Tracking Patch Third Party Advisory bugs.debian.org text/html	CONFIRM

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	All	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All

cpe:2.3:a:imagemagick:imagemagick:*:*:*:*:*:*:*:*:

cpe:2.3:a:imagemagick:imagemagick:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→