



CVE-2017-11535

Published on: 07/22/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:25 PM UTC

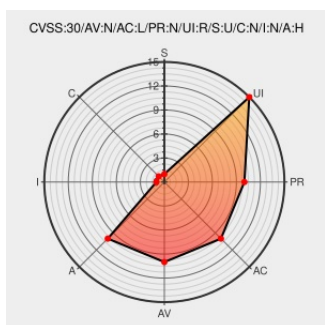
CVE-2017-11535

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Imagemagick](#) from [Imagemagick](#) contain the following vulnerability:

When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WritePSImage() function in coders/ps.c.

CVE-2017-11535 has been assigned by [M](#) 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	NONE	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
heap-overflow in GetPixelAlpha() · Issue #561 · ImageMagick/ImageMagick · GitHub	Exploit Issue Tracking Patch Third Party Advisory github.com	CONFIRM github.com/ImageMagick/ImageMagick/issues/561

[text/html](#)

Debian -- Security Information -- DSA-4019-1 imagemagick

[www.debian.org](#)
Deprecated Link
[text/html](#)

 DEBIAN DSA-4019

USN-3681-1: ImageMagick vulnerabilities | Ubuntu security notices

[usn.ubuntu.com](#)
[text/html](#)

 UBUNTU USN-3681-1

Debian -- Security Information -- DSA-4204-1 imagemagick

[www.debian.org](#)
Deprecated Link
[text/html](#)

 DEBIAN DSA-4204

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	7.0.6-1	All	All	All
Application	Imagemagick	Imagemagick	7.0.6-1	All	All	All

cpe:2.3:a:imagemagick:imagemagick:7.0.6-1:*:*:*:*:*:

cpe:2.3:a:imagemagick:imagemagick:7.0.6-1:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→