

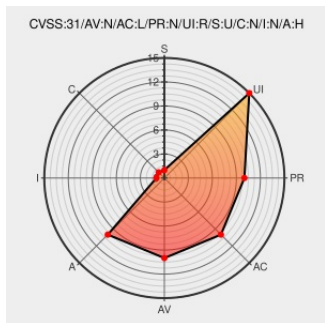


CVE-2017-17504

Published on: 12/10/2017 12:00:00 AM UTC

Last Modified on: 04/28/2021 06:08:00 PM UTC

CVE-2017-17504

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

ImageMagick before 7.0.7-12 has a coders/png.c

Magick_png_read_raw_profile heap-based buffer over-read via a crafted file, related to ReadOneMNGImage.

CVE-2017-17504 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-buffer-overflow in Magick_png_read_raw_profile · Issue #872 · ImageMagick/ImageMagick · GitHub	Exploit Patch Third Party Advisory github.com text/html	CONFIRM github.com/ImageMagick/ImageMagick/issues/872

Debian -- Security Information -- DSA-4074-1 imagemagick	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4074
[SECURITY] [DLA 1227-1] imagemagick security update	Mailing List Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20180101 [SECURITY] [DLA 1227-1] imagemagick security update
USN-3681-1: ImageMagick vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3681-1
Debian -- Security Information -- DSA-4204-1 imagemagick	Third Party Advisory 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
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All
Application	Imagemagick	Imagemagick	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:						
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:						
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→

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)