



# CVE-2017-17500

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-17500
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-12-11 02:29:00 UTC
<b>Updated</b>	2023-11-07 02:41:00 UTC
<b>Description</b>	ReadRGBImage in coders/rgb.c in GraphicsMagick 1.3.26 has a magick/import.c ImportRGBQuantumType heap-based bu

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.3.26	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.3.26	All	All	All

## References

Reference	Source	Link
Debian -- Security Information -- DSA-4321-1 graphicsmagick	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
[SECURITY] [DLA 1231-1] graphicsmagick security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 30 Update: GraphicsMagick-1.3.32-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 29 Update: GraphicsMagick-1.3.32-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: GraphicsMagick-1.3.32-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
GraphicsMagick / Bugs / #523 heap-buffer-overflow	CONFIRM	<a href="http://sourceforge.net">sourceforge.net</a>

Mercurial Repository: p/graphicsmagick/code: changeset 15285:1366f2dd9931	CONFIRM	<a href="http://hg.code.sf.net">hg.code.sf.net</a>
GraphicsMagick CVE-2017-17500 Heap-Based Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
[SECURITY] [DLA 1401-1] graphicsmagick security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 29 Update: GraphicsMagick-1.3.32-1.fc29 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
USN-4248-1: GraphicsMagick vulnerabilities   Ubuntu security notices	UBUNTU	<a href="http://usn.ubuntu.com">usn.ubuntu.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[500986](#) Alpine Linux Security Update for graphicsmagick

[504910](#) Alpine Linux Security Update for graphicsmagick

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)