



# CVE-2014-9845

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

## Summary

<b>CVE</b>	CVE-2014-9845
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-20 16:59:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	The ReadDIBImage function in coders/dib.c in ImageMagick allows remote attackers to cause a denial of service (crash) via

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.10	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.8.8-9	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.8.8-9	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Leap</a>	42.1	All	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Debuginfo</a>	11.0	sp4	All	All

Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Debuginfo</a>	11.0	sp4	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Desktop</a>	12.0	sp1	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Desktop</a>	12.0	sp1	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Server</a>	11.0	sp4	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Server</a>	12.0	sp1	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Server</a>	11.0	sp4	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Server</a>	12.0	sp1	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Software Development Kit</a>	11.0	sp4	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	sp1	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Software Development Kit</a>	11.0	sp4	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Software Development Kit</a>	12.0	sp1	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Workstation Extension</a>	12.0	sp1	All	All
Operating System	<a href="#">Opensuse Project</a>	<a href="#">Suse Linux Enterprise Workstation Extension</a>	12.0	sp1	All	All
Application	<a href="#">Suse</a>	<a href="#">Studio Onsite</a>	1.3	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Studio Onsite</a>	1.3	All	All	All

## References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2016:3060-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List,
[security-announce] openSUSE-SU-2016:1748-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List,
USN-3131-1: ImageMagick vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party
404 Not Found	CONFIRM	<a href="http://anonscm.debian.org">anonscm.debian.org</a>	Patch, Third
[security-announce] SUSE-SU-2016:1782-1: important: Security update for	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List,
[security-announce] openSUSE-SU-2016:1724-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List,
oss-security - Re: ImageMagick CVEs	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List,
[security-announce] openSUSE-SU-2016:2073-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List,
[security-announce] openSUSE-SU-2016:1833-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List,
[security-announce] SUSE-SU-2016:1783-1: important: Security update for	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List,
1343503 – (CVE-2014-9845) CVE-2014-9845 ImageMagick: crash due to corrupted dib file	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Track
[security-announce] SUSE-SU-2016:1784-1: important: Security update for	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List,
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, a

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)