



CVE-2014-9817

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-9817
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-30 15:59:00 UTC
Updated	2017-04-04 15:42:00 UTC
Description	Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted pdb file.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagemagick	Imagemagick	-	All	All	All
Application	Imagemagick	Imagemagick	-	All	All	All

References

Reference	Source	Link	Type
oss-security - Re: ImageMagick CVEs	MLIST	www.openwall.com	Misc
oss-security - Imagemagick fuzzing bug	MLIST	www.openwall.com	Misc
404 Not Found	CONFIRM	anonscm.debian.org	Proof of Concept
1343473 – (CVE-2014-9817) CVE-2014-9817 ImageMagick: heap buffer overflow in pdb file handling	CONFIRM	bugzilla.redhat.com	Issue Tracking
CVE Program record	CVE.ORG	www.cve.org	CVE Record
NVD vulnerability detail	NVD	nvd.nist.gov	CVE Record

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report