



CVE-2017-14400

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

Summary

CVE	CVE-2017-14400
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-12 21:29:00 UTC
Updated	2020-09-08 00:15:00 UTC
Description	In ImageMagick 7.0.7-1 Q16, the PersistPixelCache function in magick/cache.c mishandles the pixel cache nexus, which al

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagemagick	Imagemagick	7.0.7-1	All	All	All
Application	Imagemagick	Imagemagick	7.0.7-1	All	All	All

References

Reference	Source	Link
ImageMagick CVE-2017-14400 Denial of Service Vulnerability	BID	www.bids...
[SECURITY] [DLA 2366-1] imagemagick security update	MLIST	lists.fedoraproject.org
USN-3681-1: ImageMagick vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
[SECURITY] [DLA 1785-1] imagemagick security update	MLIST	lists.fedoraproject.org
Null Pointer Dereference in GetVirtualPixels MagickCore/cache.c:3185 · Issue #746 · ImageMagick/ImageMagick · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

Free CVE JSON API [cve.report/api](#)

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