



CVE-2019-13297

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

Summary

CVE	CVE-2019-13297
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-05 01:15:00 UTC
Updated	2020-08-19 18:59:00 UTC
Description	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage beca

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	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	10.0	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	7.0.8-50	q16	All	All
Application	Imagemagick	Imagemagick	7.0.8-50	q16	All	All
Operating System	Opensuse	Leap	15.0	All	All	All

Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source
heap-buffer-overflow at MagickCore/threshold.c:328:11 in AdaptiveThresholdImage · Issue #1609 · ImageMagick/ImageMagick · GitHub	MITRE
[security-announce] openSUSE-SU-2019:1983-1: moderate: Security update f	SUSE
USN-4192-1: ImageMagick vulnerabilities Ubuntu security notices Ubuntu	UBUNTU
[SECURITY] [DLA 2333-1] imagemagick security update	ML
Debian -- Security Information -- DSA-4712-1 imagemagick	DEBIAN
https://github.com/ImageMagick/ImageMagick/issues/1609 · ImageMagick/ImageMagick@604588f · GitHub	MITRE
[SECURITY] [DLA 1888-1] imagemagick security update	ML
https://github.com/ImageMagick/ImageMagick/issues/1609 · ImageMagick/ImageMagick6@35c7032 · GitHub	MITRE
CVE Program record	CV
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296080 Oracle Solaris 11.4 Support Repository Update (SRU) 13.4.0 Missing (CPUJUL2019)
355822 Amazon Linux Security Advisory for php71-pecl-imagick : ALAS-2023-1814
355823 Amazon Linux Security Advisory for php56-pecl-imagick : ALAS-2023-1811
355824 Amazon Linux Security Advisory for php54-pecl-imagick : ALAS-2023-1810
355828 Amazon Linux Security Advisory for php55-pecl-imagick : ALAS-2023-1812
355829 Amazon Linux Security Advisory for php70-pecl-imagick : ALAS-2023-1813
355832 Amazon Linux Security Advisory for php72-pecl-imagick : ALAS-2023-1815
357342 Amazon Linux Security Advisory for ImageMagick : ALAS-2024-1926
377297 Alibaba Cloud Linux Security Update for imagemagick (ALINUX2-SA-2020:0071)
501006 Alpine Linux Security Update for imagemagick
501012 Alpine Linux Security Update for imagemagick6

© [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](#)