



CVE-2017-12876

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

Summary

CVE	CVE-2017-12876
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-28 19:29:00 UTC
Updated	2021-04-28 17:50:00 UTC
Description	Heap-based buffer overflow in enhance.c in ImageMagick before 7.0.6-6 allows remote attackers to cause a denial of service

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
https://github.com/ImageMagick/ImageMagick/issues/663 · ImageMagick/ImageMagick@1cc6f0c · GitHub	CONFIRM	github.com
oss-security - imagemagick: heap-based buffer overflow in .omp_outlined..32 (enhance.c)	MLIST	www.openwall.com
ImageMagick: Multiple vulnerabilities (GLSA 201711-07) — Gentoo security	GENTOO	security.gentoo.org
imagemagick: heap-based buffer overflow in .omp_outlined..32 (enhance.c) agostino's blog	MISC	blogs.gentoo.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710460](#) Gentoo Linux ImageMagick Multiple Vulnerabilities (GLSA 201711-07)

© [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](#)