



# CVE-2017-5507

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

## Summary

<b>CVE</b>	CVE-2017-5507
<b>State</b>	PUBLIC
<b>Assigner</b>	security@debian.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-24 15:59:00 UTC
<b>Updated</b>	2020-10-15 16:08:00 UTC
<b>Description</b>	Memory leak in coders/mpc.c in ImageMagick before 6.9.7-4 and 7.x before 7.0.4-4 allows remote attackers to cause a den

## Risk And Classification

**Problem Types:** CWE-772

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-0	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-1	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-10	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-2	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-3	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-4	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-5	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-6	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-7	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-8	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.1-9	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-0	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-1	All	All	All



Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-0	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-1	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-10	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-2	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-3	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-4	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-5	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-6	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-7	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-8	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.2-9	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-0	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-1	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-10	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-2	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-3	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-4	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-5	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-6	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-7	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-8	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.3-9	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.4-0	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.4-1	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.4-2	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	7.0.4-3	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	All	All	All	All

## References

### Reference

oss-security - Re: CVE Request: Imagemagick: various flaws: memory corruption, out-of-bounds writes, memory leaks, double-frees, off-by-or

Debian -- Security Information -- DSA-3799-1 imagemagick

oss-security - CVE Request: Imagemagick: various flaws: memory corruption, out-of-bounds writes, memory leaks, double-frees, off-by-one er

ImageMagick/ChangeLog at 6.9.7-4 · ImageMagick/ImageMagick · GitHub

#851382 - imagemagick: CVE-2017-5507: coders/mpc.c: memory leak in mpc file handling - Debian Bug report logs

ImageMagick CVE-2017-5507 Local Information Disclosure Vulnerability

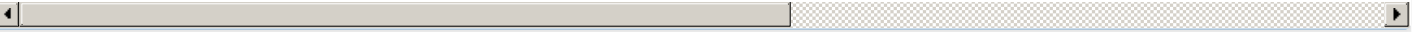
ImageMagick: Multiple vulnerabilities (GLSA 201702-09) — Gentoo Security

ImageMagick/ChangeLog at 7.0.4-4 · ImageMagick/ImageMagick · GitHub

... · ImageMagick/ImageMagick@66e283e · GitHub

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[710493](#) Gentoo Linux ImageMagick Multiple Vulnerabilities (GLSA 201702-09)

© [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](#)