



# CVE-2005-0005

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

## Summary

<b>CVE</b>	CVE-2005-0005
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-05-02 04:00:00 UTC
<b>Updated</b>	2017-10-11 01:29:00 UTC
<b>Description</b>	Heap-based buffer overflow in psd.c for ImageMagick 6.1.0, 6.1.7, and possibly earlier versions allows remote attackers to

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## 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>	3.0	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ppc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	sparc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	m68k	All

Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ppc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	sparc	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.5	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.7	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.1a	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.2	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc1	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc2	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc3	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.5	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.7	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.1a	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.2	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc1	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc2	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc3	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.0	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.0.6	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.1	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.1.3	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.1.4	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.0	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.0.6	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.1	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.1.3	All	All	All
Application	<a href="#">Graphicsmagick</a>	<a href="#">Graphicsmagick</a>	1.1.4	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	5.3.3	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	5.4.3	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	5.4.7	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.0	All	All	All



Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.1.2	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.1.3	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.1.4	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.1.5	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.1.6	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.1.7	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.2	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.2.0.4	All	All	All
Application	<a href="#">Imagemagick</a>	<a href="#">Imagemagick</a>	6.2.0.7	All	All	All
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	3.0	All	All	All
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	3.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	i386	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	x86_64	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.0	All	i386	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	8.2	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.0	All	x86_64	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.1	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	9.2	All	All	All

## References

Reference	Source	Link	Tags
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>	
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	Patch
Gentoo Linux Documentation -- GraphicsMagick: PSD decoding heap overflow	GENTOO	<a href="http://www.gentoo.org">www.gentoo.org</a>	
Debian -- Security Information -- DSA-646-1 imagemagick	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Patch, Vendor Advisory
rhn.redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>	
Accenture   Let there be change	IDEFENSE	<a href="http://www.idefense.com">www.idefense.com</a>	Exploit

'[USN-62-1] imagemagick vulnerability' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)