



CVE-2006-4144

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

Summary

CVE	CVE-2006-4144
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-15 23:04:00 UTC
Updated	2018-10-17 21:33:00 UTC
Description	Integer overflow in the ReadSGIImage function in sgi.c in ImageMagick before 6.2.9 allows user-assisted attackers to cause a denial of service (crash) or execute arbitrary code.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagemagick	Imagemagick	6.0.1	All	All	All
Application	Imagemagick	Imagemagick	6.0.2	All	All	All
Application	Imagemagick	Imagemagick	6.0.2.5	All	All	All
Application	Imagemagick	Imagemagick	6.0.3	All	All	All
Application	Imagemagick	Imagemagick	6.0.4	All	All	All
Application	Imagemagick	Imagemagick	6.0.5	All	All	All
Application	Imagemagick	Imagemagick	6.0.6	All	All	All
Application	Imagemagick	Imagemagick	6.0.7	All	All	All
Application	Imagemagick	Imagemagick	6.0.8	All	All	All
Application	Imagemagick	Imagemagick	6.1	All	All	All
Application	Imagemagick	Imagemagick	6.1.1.6	All	All	All
Application	Imagemagick	Imagemagick	6.1.2	All	All	All
Application	Imagemagick	Imagemagick	6.1.3	All	All	All
Application	Imagemagick	Imagemagick	6.1.4	All	All	All
Application	Imagemagick	Imagemagick	6.1.5	All	All	All
Application	Imagemagick	Imagemagick	6.1.6	All	All	All
Application	Imagemagick	Imagemagick	6.1.7	All	All	All

[illegible]

Application	Imagemagick	Imagemagick	6.2.4	All	All	All
Application	Imagemagick	Imagemagick	6.2.4.5	All	All	All
Application	Imagemagick	Imagemagick	6.2.5	All	All	All
Application	Imagemagick	Imagemagick	6.2.6	All	All	All
Application	Imagemagick	Imagemagick	6.2.7	All	All	All
Application	Imagemagick	Imagemagick	6.2.8	All	All	All

References						
Reference						Source
Gentoo update for imagemagick - Advisories - Secunia						SECUNIA
SecurityFocus						BUGTRAQ
ImageMagick "ReadSGIImage()" Integer Overflow Vulnerability - Advisories - Secunia						SECUNIA
IBM X-Force Exchange						XF
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia						SECUNIA
usn/usn-337-1 - Ubuntu: Linux for human beings						UBUNTU
SecurityReason - ImageMagick ReadSGIImage() Heap Overflow						SREASON
ImageMagick SGI Image File Remote Heap Buffer Overflow Vulnerability						BID
Gentoo Linux Documentation -- ImageMagick: Multiple Vulnerabilities						GENTOO
rPath update for ImageMagick - Secunia.com						SECUNIA
Red Hat update for ImageMagick - Advisories - Secunia						SECUNIA
Debian -- Security Information -- DSA-1213-1 imagemagick						DEBIAN
SUSE update for ImageMagick - Secunia Advisories - Vulnerability Intelligence - Secunia.com						SECUNIA
Advisories - Mandriva Linux						MANDRIVA
404 Not Found						MISC
20060901-01-P						SGI
Mandriva update for ImageMagick - Advisories - Secunia						SECUNIA
Debian update for imagemagick - Advisories - Secunia						SECUNIA
Security Announcement						SUSE
rhn.redhat.com Red Hat Support						REDHAT
[#RPL-605] Multiple vulnerabilities in ImageMagick: CVE-2006-3743 CVE-2006-3744 CVE-2006-4144 - rPath JIRA						CONFIRM
SecurityFocus						BUGTRAQ
Ubuntu update for imagemagick - Secunia Advisories - Vulnerability Intelligence - Secunia.com						SECUNIA
SecurityTracker.com Archives - ImageMagick ReadSGIImage() Heap Overflow Lets Remote Users Execute Arbitrary Code						SECTrack
Repository / Oval Repository						OVAL
CVE Program record						CVE.ORG
NVD vulnerability detail						NVD

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.
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](#)