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

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

Application	Imagemagick	Imagemagick	6.1.8	All	All	All
Application	Imagemagick	Imagemagick	6.2	All	All	All
Application	Imagemagick	Imagemagick	6.2.0.4	All	All	All
Application	Imagemagick	Imagemagick	6.2.0.7	All	All	All
Application	Imagemagick	Imagemagick	6.2.1	All	All	All
Application	Imagemagick	Imagemagick	6.2.2	All	All	All
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
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
Application	Imagemagick	Imagemagick	6.1.8	All	All	All
Application	Imagemagick	Imagemagick	6.2	All	All	All
Application	Imagemagick	Imagemagick	6.2.0.4	All	All	All
Application	Imagemagick	Imagemagick	6.2.0.7	All	All	All
Application	Imagemagick	Imagemagick	6.2.1	All	All	All
Application	Imagemagick	Imagemagick	6.2.2	All	All	All

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

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.