CVE-2006-3743

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2006-3743
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-25 01:04:00 UTC
Updated	2017-10-11 01:31:00 UTC
Description	Multiple buffer overflows in ImageMagick before 6.2.9 allow user-assisted attackers to execute arbitrary code via crafted XC

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	6.2	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	6.2.0.8	All	All	All
Application	Imagemagick	Imagemagick	6.2.1	All	All	All
Application	Imagemagick	Imagemagick	6.2.1.7	All	All	All
Application	Imagemagick	Imagemagick	6.2.2	All	All	All
Application	Imagemagick	Imagemagick	6.2.2.5	All	All	All
Application	Imagemagick	Imagemagick	6.2.3	All	All	All
Application	Imagemagick	Imagemagick	6.2.3.6	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	6.2	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	6.2.0.8	All	All	All
Application	Imagemagick	Imagemagick	6.2.1	All	All	All
Application	Imagemagick	Imagemagick	6.2.1.7	All	All	All
Application	Imagemagick	Imagemagick	6.2.2	All	All	All
Application	Imagemagick	Imagemagick	6.2.2.5	All	All	All
Application	Imagemagick	Imagemagick	6.2.3	All	All	All
Application	Imagemagick	Imagemagick	6.2.3.6	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
Gentoo update for imagemagick - Advisories - Secunia
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia
Gentoo Linux Documentation -- ImageMagick: Multiple Vulnerabilities
Repository / Oval Repository
rPath update for ImageMagick - Secunia.com
Webmail - OVH
Red Hat update for ImageMagick - Advisories - Secunia
usn/usn-340-1 - Ubuntu: Linux for human beings
Debian -- Security Information -- DSA-1168-1 imagemagick
IBM X-Force Exchange
Ubuntu update for imagemagick - Advisories - Secunia
SecurityTracker.com Archives - ImageMagick Integer/Buffer Overflows in Processing XCF and Sun Bitmap Images Lets Remote Users Execu
SUSE update for ImageMagick - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Advisories - Mandriva Linux
144854 – media-gfx/imagemagick: heap and stack buffer overflow (CVE-2006-374{3|4})
28205
20060901-01-P

Mandriva update for ImageMagick - Advisories - Secunia
Security Announcement
rhn.redhat.com | Red Hat Support
[#RPL-605] Multiple vulnerabilities in ImageMagick: CVE-2006-3743 CVE-2006-3744 CVE-2006-4144 - rPath JIRA
ImageMagick XCF Image File Remote Unspecified Buffer Overflow Vulnerability
ImageMagick XCF and Sun Rasterfile Buffer Overflows - Advisories - Secunia
Debian update for imagemagick - Secunia.com
CVE Program record
NVD vulnerability detail

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.