CVE-2005-0397

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

Summary

CVE	CVE-2005-0397
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Format string vulnerability in the SetImageInfo function in image.c for ImageMagick before 6.0.2.5 may allow remote attacke

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagemagick	Imagemagick	5.2	All	All	All

Application	Imagemagick	Imagemagick	5.3	All	All	All
Application	Imagemagick	Imagemagick	5.4	All	All	All
Application	Imagemagick	Imagemagick	5.5	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
Gentoo Linux Documentation -- ImageMagick: Filename handling vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.gento
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecu
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.x
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redha
Gentoo Bug 83542 - media-gfx/imagemagick: filename handling format string bug.	af854a3a-2127-422b-91ae-364da2661108	bugs.gento
Security Announcement	af854a3a-2127-422b-91ae-364da2661108	www.novell
'[USN-90-1] Imagemagick vulnerability' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redha
Debian -- Security Information -- DSA-702-1 imagemagick	af854a3a-2127-422b-91ae-364da2661108	www.debia
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

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