CVE-2007-4987

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

Summary

CVE	CVE-2007-4987
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-24 22:17:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Off-by-one error in the ReadBlobString function in blob.c in ImageMagick before 6.3.5-9 allows context-dependent attackers

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Imagemagick	Imagemagick	5.3.3	All	All	All

Application	Imagemagick	Imagemagick	5.3.8	All	All	All
Application	Imagemagick	Imagemagick	5.4.2.3	All	All	All
Application	Imagemagick	Imagemagick	5.4.3	All	All	All
Application	Imagemagick	Imagemagick	5.4.4.5	All	All	All
Application	Imagemagick	Imagemagick	5.4.7	All	All	All
Application	Imagemagick	Imagemagick	5.4.8	All	All	All
Application	Imagemagick	Imagemagick	5.4.8.2_1.1.0	All	All	All
Application	Imagemagick	Imagemagick	5.5.3_.2_1.2.0	All	All	All
Application	Imagemagick	Imagemagick	5.5.4	All	All	All
Application	Imagemagick	Imagemagick	5.5.6	All	All	All
Application	Imagemagick	Imagemagick	5.5.6.0_20030409	All	All	All
Application	Imagemagick	Imagemagick	5.5.7	All	All	All
Application	Imagemagick	Imagemagick	5.5.7.15	All	All	All
Application	Imagemagick	Imagemagick	6.0	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	6.0.4.4	All	All	All
Application	Imagemagick	Imagemagick	6.0.5	All	All	All
Application	Imagemagick	Imagemagick	6.0.6	All	All	All
Application	Imagemagick	Imagemagick	6.0.6.2	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	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	6.2.0.3	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	6.2.3	All	All	All
Application	Imagemagick	Imagemagick	6.2.3.4	All	All	All
Application	Imagemagick	Imagemagick	6.2.4	All	All	All
Application	Imagemagick	Imagemagick	6.2.4.3	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	6.2.9	All	All	All
Application	Imagemagick	Imagemagick	6.2.9.2	All	All	All
Application	Imagemagick	Imagemagick	6.3.1	All	All	All
Application	Imagemagick	Imagemagick	6.3.2	All	All	All
Application	Imagemagick	Imagemagick	6.3.3_3	All	All	All
Application	Imagemagick	Imagemagick	6.3.3_5	All	All	All
Application	Imagemagick	Imagemagick	6.3.3_6	All	All	All
Application	Imagemagick	Imagemagick	6.3.4	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Debian -- Security Information -- DSA-1858-1 imagemagick	af854a3a-2127-422b-91ae-364
ImageMagick Multiple Vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-91ae-364
Advisories | Mandriva	af854a3a-2127-422b-91ae-364
[Magick-announce] ImageMagick 6.3.5-9, important security updates	af854a3a-2127-422b-91ae-364
Security Announcement	af854a3a-2127-422b-91ae-364
rPath update for ImageMagick - Advisories - Secunia	af854a3a-2127-422b-91ae-364
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364
ImageMagick: Multiple vulnerabilities — Gentoo Linux Documentation	af854a3a-2127-422b-91ae-364
ImageMagick Off-by-one and Integer Overflows Let Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364

SecurityFocus	af854a3a-2127-422b-91ae-364
USN-523-1: ImageMagick vulnerabilities | Ubuntu	af854a3a-2127-422b-91ae-364
ImageMagick: Changelog	af854a3a-2127-422b-91ae-364
Gentoo Bug 186030 - media-gfx/imagemagick < 6.3.5.9: Multiple vulnerabilities (CVE-2007-498{5,6,7,8})	af854a3a-2127-422b-91ae-364
ImageMagick Blob.C Off-By-One Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364
Ubuntu update for imagemagick - Advisories - Secunia	af854a3a-2127-422b-91ae-364
labs.idefense.com/intelligence/vulnerabilities/display.php	af854a3a-2127-422b-91ae-364
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364
SUSE Update for Multiple Packages - Advisories - Secunia	af854a3a-2127-422b-91ae-364
Mandriva update for ImageMagick - Advisories - Secunia	af854a3a-2127-422b-91ae-364
Gentoo update for imagemagick - Advisories - Secunia	af854a3a-2127-422b-91ae-364
issues.rpath.com/browse/RPL-1743	af854a3a-2127-422b-91ae-364
Debian update for imagemagick - Secunia.com	af854a3a-2127-422b-91ae-364
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-12-05	Mark J Cox	Note: As the address of the overwritten byte is not under attacker’s control, the worst impact his

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