CVE-2016-6520

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

Summary

CVE	CVE-2016-6520
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-13 15:59:10 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Buffer overflow in MagickCore/enhance.c in ImageMagick before 7.0.2-7 allows remote attackers to have unspecified impac

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

EPSS: 0.034170000 probability, percentile 0.875230000 (date 2026-05-11)

Problem Types: CWE-125 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
2.0	nvd@nist.gov	Primary	6.4		AV:N/AC:L/Au:N/C:P/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

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

References

Reference
ImageMagick Buffer Overflow in ContrastStretchImage() Lets Remote Users Obtain Potentially Sensitive Information and Deny Service - Secu
oss-security - CVE Request ImageMagick buffer overflow
oss-security - Re: CVE Request ImageMagick buffer overflow
ImageMagick: Changelog
Evaluate lazy pixel cache morphology to prevent buffer overflow (bug … · ImageMagick/ImageMagick@76401e1 · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**