ImageMagick: Heap-use-after-free via XMP profile could result in a crash when printing values

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

Summary

CVE	CVE-2026-40311
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 22:16:29 UTC
Updated	2026-04-13 22:16:29 UTC
Description	ImageMagick is free and open-source software used for editing and manipulating digital images. Versions below 7.1.2-19 a

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from security-advisories@github.com

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

Problem Types: CWE-416 | CWE-693 | CWE-416 CWE-416: Use After Free | CWE-693 CWE-693: Protection Mechanism Failure

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ImageMagick	ImageMagick	affected < 7.1.2-19	Not specified
CNA	ImageMagick	ImageMagick	affected < 6.9.13-44	Not specified

References

Reference	Source	Link	Tags
github.com/dlemstra/Magick.NET/releases/tag/14.12.0	security-advisories@github.com	github.com	
github.com/ImageMagick/ImageMagick/security/advisories/GHSA-r83h-crwp-3vm7	security-advisories@github.com	github.com	
github.com/ImageMagick/ImageMagick/commit/5facfecf1abb3fed46a08f614dcc43...	security-advisories@github.com	github.com	
github.com/ImageMagick/ImageMagick/releases/tag/7.1.2-19	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

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