



CImg Library: Integer overflow in PNM size check bypasses memory guard (_load_pnm)

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-42144
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 18:16:31 UTC
Updated	2026-05-07 15:43:39 UTC
Description	CImg Library is a C++ library for image processing. Prior to commit 4ca26bc, there is an integer overflow vulnerability in the

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from security-advisories@github.com

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

EPSS: 0.000130000 probability, percentile 0.019690000 (date 2026-05-12)

Problem Types: CWE-190 | CWE-190 CWE-190: Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GreycLab	Clmg	affected < 4ca26bce4d8c61fcd1507d5f9401b9fb1222c27d	Not specified

References

Reference	Source	Link	Tags
github.com/GreycLab/Clmg/releases/tag/v.3.7.5	security-advisories@github.com	github.com	
github.com/GreycLab/Clmg/security/advisories/GHSA-4663-63fm-44gc	security-advisories@github.com	github.com	
github.com/GreycLab/Clmg/issues/478	security-advisories@github.com	github.com	
github.com/GreycLab/Clmg/commit/4ca26bce4d8c61fcd1507d5f9401b9fb1222c27d	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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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