



LIBPNG has a use-after-free in png_set_PLTE, png_set_tRNS and png_set_hIST leading to corrupted chunk data and potential heap information disclosure

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

Summary

CVE CVE-2026-34757**State** PUBLISHED**Assigner** GitHub_M**Source Priority** CVE Program / NVD first with legacy fallback**Published** 2026-04-09 15:16:11 UTC**Updated** 2026-04-13 15:02:47 UTC**Description** LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) ra

Risk And Classification

Primary CVSS: v3.1 5.1 MEDIUM from security-advisories@github.com**CVSS:** 3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N**EPSS:** 0.000160000 probability, percentile 0.034620000 (date 2026-04-15)**Problem Types:** CWE-416 | CWE-416 CWE-416: Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	5.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pnggroup	Libpng	affected >= 1.0.9, < 1.6.57	Not specified

References

Reference	Source	Link	Tag
github.com/pnggroup/libpng/issues/836	security-advisories@github.com	github.com	
github.com/pnggroup/libpng/commit/398cbe3df03f4e11bb031e07f416dfdde3684e8a	security-advisories@github.com	github.com	
github.com/pnggroup/libpng/security/advisories/GHSA-6fr7-g8h7-v645	security-advisories@github.com	github.com	
github.com/pnggroup/libpng/commit/55d20aaa322c9274491cda82c5cd4f99b48c6bcc	security-advisories@github.com	github.com	
github.com/pnggroup/libpng/issues/837	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

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