



# LIBPNG has use-after-free via pointer aliasing in `png\_set\_tRNS` and `png\_set\_PLTE`

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

## Summary

<b>CVE</b>	CVE-2026-33416
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 17:16:38 UTC
<b>Updated</b>	2026-04-02 20:28:33 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 7.5 HIGH from security-advisories@github.com

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

**EPSS:** 0.000510000 probability, percentile 0.158320000 (date 2026-04-01)

**Problem Types:** CWE-416 | CWE-416 CWE-416: Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pnggroup	Libpng	affected >= 1.2.1, < 1.6.56	Not specified

### References

Reference	Source	Link	Type
github.com/pnggroup/libpng/commit/23019269764e35ed8458e517f1897bd3c54820eb	security-advisories@github.com	github.com	Patch
github.com/pnggroup/libpng/security/advisories/GHSA-m4pc-p4q3-4c7j	security-advisories@github.com	github.com	Patch
github.com/pnggroup/libpng/commit/a3a21443ed12bfa1ef46fa0d4fb2b74a0fa34a25	security-advisories@github.com	github.com	Patch
github.com/pnggroup/libpng/commit/c1b0318b393c90679e6fa5bc1d329fd5d5012ec1	security-advisories@github.com	github.com	Patch
github.com/pnggroup/libpng/pull/824	security-advisories@github.com	github.com	Issue
github.com/pnggroup/libpng/commit/7ea9eea884a2328cc7fdb3c0c00246a50d90667	security-advisories@github.com	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	Card
NVD vulnerability detail	NVD	nvd.nist.gov	Card

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.

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)