pnggroup libpng pnm2png pnm2png.c do_pnm2png heap-based overflow

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

Summary

CVE	CVE-2026-3713
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-08 06:16:11 UTC
Updated	2026-04-22 21:27:27 UTC
Description	A flaw has been found in pnggroup libpng up to 1.6.55. Affected by this vulnerability is the function do_pnm2png of the file c

Risk And Classification

Primary CVSS: v4.0 4.8 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000170000 probability, percentile 0.040690000 (date 2026-04-22)

Problem Types: CWE-119 | CWE-122 | CWE-122 Heap-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:C
3.0	CNA	DECLARED	5.3	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:C
2.0	cna@vuldb.com	Secondary	4.3		AV:L/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	4.3		AV:L/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:ND/RC:C

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:C

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pnggroup	Libpng	affected 1.6.0	Not specified
CNA	Pnggroup	Libpng	affected 1.6.1	Not specified
CNA	Pnggroup	Libpng	affected 1.6.2	Not specified
CNA	Pnggroup	Libpng	affected 1.6.3	Not specified
CNA	Pnggroup	Libpng	affected 1.6.4	Not specified
CNA	Pnggroup	Libpng	affected 1.6.5	Not specified
CNA	Pnggroup	Libpng	affected 1.6.6	Not specified
CNA	Pnggroup	Libpng	affected 1.6.7	Not specified
CNA	Pnggroup	Libpng	affected 1.6.8	Not specified
CNA	Pnggroup	Libpng	affected 1.6.9	Not specified
CNA	Pnggroup	Libpng	affected 1.6.10	Not specified
CNA	Pnggroup	Libpng	affected 1.6.11	Not specified
CNA	Pnggroup	Libpng	affected 1.6.12	Not specified
CNA	Pnggroup	Libpng	affected 1.6.13	Not specified
CNA	Pnggroup	Libpng	affected 1.6.14	Not specified
CNA	Pnggroup	Libpng	affected 1.6.15	Not specified
CNA	Pnggroup	Libpng	affected 1.6.16	Not specified
CNA	Pnggroup	Libpng	affected 1.6.17	Not specified
CNA	Pnggroup	Libpng	affected 1.6.18	Not specified

CNA	Pnggroup	Libpng	affected 1.6.19	Not specified
CNA	Pnggroup	Libpng	affected 1.6.20	Not specified
CNA	Pnggroup	Libpng	affected 1.6.21	Not specified
CNA	Pnggroup	Libpng	affected 1.6.22	Not specified
CNA	Pnggroup	Libpng	affected 1.6.23	Not specified
CNA	Pnggroup	Libpng	affected 1.6.24	Not specified
CNA	Pnggroup	Libpng	affected 1.6.25	Not specified
CNA	Pnggroup	Libpng	affected 1.6.26	Not specified
CNA	Pnggroup	Libpng	affected 1.6.27	Not specified
CNA	Pnggroup	Libpng	affected 1.6.28	Not specified
CNA	Pnggroup	Libpng	affected 1.6.29	Not specified
CNA	Pnggroup	Libpng	affected 1.6.30	Not specified
CNA	Pnggroup	Libpng	affected 1.6.31	Not specified
CNA	Pnggroup	Libpng	affected 1.6.32	Not specified
CNA	Pnggroup	Libpng	affected 1.6.33	Not specified
CNA	Pnggroup	Libpng	affected 1.6.34	Not specified
CNA	Pnggroup	Libpng	affected 1.6.35	Not specified
CNA	Pnggroup	Libpng	affected 1.6.36	Not specified
CNA	Pnggroup	Libpng	affected 1.6.37	Not specified
CNA	Pnggroup	Libpng	affected 1.6.38	Not specified
CNA	Pnggroup	Libpng	affected 1.6.39	Not specified
CNA	Pnggroup	Libpng	affected 1.6.40	Not specified
CNA	Pnggroup	Libpng	affected 1.6.41	Not specified
CNA	Pnggroup	Libpng	affected 1.6.42	Not specified
CNA	Pnggroup	Libpng	affected 1.6.43	Not specified
CNA	Pnggroup	Libpng	affected 1.6.44	Not specified
CNA	Pnggroup	Libpng	affected 1.6.45	Not specified
CNA	Pnggroup	Libpng	affected 1.6.46	Not specified
CNA	Pnggroup	Libpng	affected 1.6.47	Not specified
CNA	Pnggroup	Libpng	affected 1.6.48	Not specified
CNA	Pnggroup	Libpng	affected 1.6.49	Not specified
CNA	Pnggroup	Libpng	affected 1.6.50	Not specified
CNA	Pnggroup	Libpng	affected 1.6.51	Not specified
CNA	Pnggroup	Libpng	affected 1.6.52	Not specified
CNA	Pnggroup	Libpng	affected 1.6.53	Not specified

CNA	Pnggroup	Libpng	affected 1.6.54	Not specified
CNA	Pnggroup	Libpng	affected 1.6.55	Not specified

References

Reference	Source	Link	Tags
github.com/pnggroup/libpng/issues/794	cna@vuldb.com	github.com	
vuldb.com	cna@vuldb.com	vuldb.com	
vuldb.com	cna@vuldb.com	vuldb.com	
vuldb.com	cna@vuldb.com	vuldb.com	
github.com/pnggroup/libpng	cna@vuldb.com	github.com	
github.com/biniamf/pocs/tree/main/pnm2png	cna@vuldb.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: biniam (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-07T00:00:00.000Z	Advisory disclosed
CNA	2026-03-07T01:00:00.000Z	VulDB entry created
CNA	2026-03-07T11:57:28.000Z	VulDB entry last update

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