



CVE-2015-7700

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

Summary

CVE	CVE-2015-7700
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-31 22:29:00 UTC
Updated	2017-09-05 18:11:00 UTC
Description	Double-free vulnerability in the sPLT chunk structure and png.c in pngcrush before 1.7.87 allows attackers to have unspecified

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pngcrush Project	Pngcrush	All	All	All	All

References

Reference	Source	Link	Tags
Pngcrush change log and "to do"	CONFIRM	pmt.sourceforge.net	Broken Link
PNG and MNG tools / News: pngcrush-1.7.87 released	CONFIRM	sourceforge.net	Release Notes
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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