libpng

libpng is the official PNG reference library. It supports almost all PNG features, is extensible, and has been extensively tested for over 20 years. The home site for development versions (i.e., may be buggy or subject to change or include experimental features) is http://libpng.sourceforge.net/, and the place to go for questions about the library is the png-mng-implement mailing list.

libpng is available as ANSI C (C89) source code and requires zlib 1.0.4 or later (1.2.5 or later recommended for performance and security reasons). The current public release, libpng 1.6.19, has fixes for two security vulnerabilities, as noted below, and includes a large number of code-quality improvements.

Vulnerability Warning

Virtually all libpng versions through 1.6.18, 1.5.23, 1.4.16, 1.2.53, and 1.0.63, respectively, have a potential out-of-bounds read in `png_set_tIME()/png_convert_to_rfc1123()` and an out-of-bounds write in `png_get_PLTE()/png_set_PLTE()`. The former vulnerability has been assigned ID CVE-2015-7981 and the latter CVE-2015-8126. Both are fixed in versions 1.6.19, 1.5.24, 1.4.17, 1.2.54, and 1.0.64, released on 12 November 2015.

Portability Note

The libpng 1.5.x and 1.6.x series continue the evolution of the libpng API, finally hiding the contents of the venerable and hoary **`png_struct`** and **`png_info`** data structures inside private (i.e., non-installed) header files. Instead of direct struct-access, applications should be using the various `png_get_xxx()` and `png_set_xxx()` accessor functions, which have existed for almost as long as libpng itself.

The above should not come as a particular surprise to anyone who has added libpng support to an application this millenium; the manual has warned of it since at least July 2000. (Specifically: *"Starting with version 2.0.0, both structures are going to be hidden, and the contents of the structures will only be accessible through the png_get/png_set functions."* OK, so the version number was off a bit...and the grammar, too, but who's counting?) Those who are happy with the current level of PNG support in their apps need not panic, however; libpng 1.2.x will continue to get security fixes for the foreseeable future. (1.0.x has gotten them for more than a decade even though Greg no longer bothers to list that series here.)

The 1.5.x and later series also include a new, more thorough test program (`pngvalid.c`) and a new `pnglibconf.h` header file that tracks what features were enabled or disabled when libpng was built. On the other hand, they no longer internally include the `zlib.h` header file, so applications that formerly depended on `png.h` to provide that will now need to include it explicitly. Complete differences relative to libpng 1.4.x are detailed here.

See the bottom of this page for warnings about other security and crash bugs in versions up through libpng 1.6.15 (and 1.2.49).

In addition to the main library sources, both the 1.4.x/1.5.x/1.6.x series and the older libpng 1.2.54 include the rpng, rpng2 and wpng demo programs, the pngminus demo

program, a subset of Willem van Schaik's PngSuite test images, and Willem's VisualPng demo program.

Current version:	1.6.19
Authors:	Guy Eric Schalnat, Andreas Dilger, John Bowler, Glenn Randers-Pehrson (current maintainer), and others
License:	Open Source
Platforms:	Unix, DOS, OS/2, Windows, Mac OS, BeOS, Amiga, etc.
README:	local web site http://www.libpng.org/pub/png/src/ http://prdownloads.sourceforge.net/libpng/ ftp://ftp.simplesystems.org/pub/libpng/png/src/libpng16/
Manual:	plain text format PDF format (version 1.4.0 [Jan 2010], courtesy of Alex Yau)
Mailing list:	png-mng-implement

Source code:	prdownloads.sourceforge.net .tar.xz .tar.gz .zip
	ftp.simplesystems.org .tar.xz .tar.gz .zip
	download.sourceforge.net .tar.xz .tar.gz .zip
	archive sizes (bytes): *941280 1411477 1257436*
	
	MD5 checksums:
	
	`3121bdc77c365a87e054b9f859f421fe libpng-1.6.19.tar.gz`
	`1e6a458429e850fc93c1f3b6dc00a48f libpng-1.6.19.tar.xz`
	`ff0e82b4d8516daa7ed6b1bf93acca48 lpng1619.zip`

Beta code:	http://libpng.sourceforge.net/ *git repository:* *access*: git://git.code.sf.net/p/libpng/code *browse*: http://sourceforge.net/p/libpng/code/ci/libpng16/tree/
Current binaries:	*operating system* *platform* *version* *(these are "unofficial" binaries compiled by third parties)*
	operating system *platform* *version* Mac OS X x86,PowerPC 1.6.18-

Previous binaries:	Linux (.rpm) (dev)	many	1.6.18-
	Linux (.rpm)	many	1.6.18-
	HP-UX	PA-RISC,IA64	1.6.18-
	FreeBSD/i386 (.txz)	x86	1.6.18
	FreeBSD/amd64 (.txz)	x86_64	1.6.18
	(these are "unofficial" binaries compiled by third parties)		
Old binaries:	*operating system*	*platform*	*version*
	Linux (.deb)	many	1.6.16-
	Linux (.txz)	x86	1.6.16-
	Linux (.txz)	x86_64	1.6.16-
	Mac OS X	x86,x86_64	1.5.4-
	(these are "unofficial" binaries compiled by third parties)		
Supporting libraries and tools:	zlib XZ *(needed only to decompress tar.xz source archive)*		

Previous series:	1.2.54
README:	local web site http://www.libpng.org/pub/png/src/ http://prdownloads.sourceforge.net/libpng/ ftp://ftp.simplesystems.org/pub/libpng/png/src/libpng12/
Manual:	plain text format HTML format (version 1.2.5 [Oct 2002], courtesy of Deron Meranda), with German translation (courtesy of Richard Krüger) MS Word format (version 1.2.0 [Sept 2001], courtesy of Pierre Delaage)

Source code:	*with config script* / *without config script*
	prdownloads.sourceforge.net .tar.xz .tar.gz .tar.xz .tar.gz .zip
	ftp.simplesystems.org .tar.xz .tar.gz .tar.xz .tar.gz .zip
	download.sourceforge.net .tar.xz .tar.gz .tar.xz .tar.gz .zip
	archive sizes (bytes): *571448* *884233* *347168* *543348* *662854*
	
	MD5 checksums:
	`2566320391ba14c2bd44081be4563cc4 libpng-1.2.54-no-config.tar.gz`
	`e8fb46f45515f1a7c3d99b7c110b485a libpng-1.2.54-no-config.tar.xz`
	`a79c19f0e29ef109f5079c7fe49ae2ad libpng-1.2.54.tar.gz`
	`bbb7a7264f1c7d9c444fd16bf6f89832 libpng-1.2.54.tar.xz`
	`daf081ede17fff3def5e0a00653e7176 lpng1254.zip`

(Almost)	*operating system* *platform* *version*

Current binaries:	*(these are "unofficial" binaries compiled by third parties)*		
Previous binaries:	*operating system* Mac OS X	*platform* x86,PowerPC	*version* 1.2.53-
	(these are "unofficial" binaries compiled by third parties)		
Old binaries:	*operating system* Linux (.rpm) (libpng3, dev) Linux (.deb) Linux (.rpm) (libpng3, dev) GnuWin32 SCO OpenServer 5 Windows CE	*platform* many many many x86 x86 many	*version* 1.2.52- 1.2.50- 1.2.49- 1.2.37- 1.2.4 1.2.3
	(these are "unofficial" binaries compiled by third parties)		

Security and Crash Bugs in Older Versions

Vulnerability Warning

libpng versions 1.6.9 through 1.6.15 (and some subset of versions up through 1.5.20) have an integer-overflow vulnerability in `png_combine_row()` when decoding very wide interlaced images, which can allow an attacker to overwrite an arbitrary amount of memory with arbitrary (attacker-controlled) data. This vulnerability has been assigned ID CVE-2014-9495 and is fixed in versions 1.6.16 and 1.5.21, released on 21 December 2014.

Vulnerability Warning

Virtually all libpng versions through 1.6.14, 1.5.19, 1.4.13, 1.2.51, and 1.0.61, respectively, have an out-of-bounds memory access in `png_user_version_check()`. It is unclear whether this could lead to an actual exploit. The bug is fixed in versions 1.6.15, 1.5.20, etc., released on 20 November 2014.

Vulnerability Warning

libpng versions 1.6.0 through 1.6.9 hang when reading images that have zero-length IDAT chunks with the progressive (streaming) reader; a malicious web site could use this bug to cause a (minor) denial of service. This vulnerability has been assigned ID CVE-2014-0333 and is fixed in version 1.6.10, released 6 March 2014.

Vulnerability Warning

libpng versions 1.6.1 through 1.6.7 fail to reject colormapped images with empty palettes, leading to a null-pointer dereference (crash) in `png_do_expand_palette()`. This vulnerability has been assigned ID CVE-2013-6954 and is fixed in version 1.6.8, released 19 December 2013.

Vulnerability Warning

Various versions of libpng through 1.5.11, 1.4.11, 1.2.49, and 1.0.59, respectively, set the top-level archive-extraction directory's permissions to be world-writable as part of the `distcheck` Makefile target's operations (`configure`-generated Makefile only). This could allow a local attacker on the build host to silently replace the extracted libpng library with a malicious version, conceivably poisoning an official binary distribution of libpng (though the likelihood of this seems remote), but more generally allowing the attacker to execute arbitrary commands with the permissions of the user running make. This vulnerability has been assigned ID CVE-2012-3386 and is fixed in version 1.5.12 (and versions 1.4.12, 1.2.50, and 1.0.60, respectively, on the older branches), released 10 July 2012.

Vulnerability Warning

All "modern" versions of libpng through 1.5.9, 1.4.10, 1.2.48, and 1.0.58, respectively, fail to correctly handle `malloc()` failure for text chunks (in `png_set_text_2()`), which can lead to memory corruption and the possibility of execution of hostile code. This serious vulnerability has been assigned ID CVE-2011-3048 and is fixed in version 1.5.10 (and versions 1.4.11, 1.2.49, and 1.0.59, respectively, on the older branches), released 29 March 2012.

Vulnerability Warning

All versions of libpng from 1.0.6 through 1.5.8, 1.4.8, 1.2.46, and 1.0.56, respectively, fail to correctly validate a heap allocation in `png_decompress_chunk()`, which can lead to a buffer-overrun and the possibility of execution of hostile code on 32-bit systems. This serious vulnerability has been assigned ID CVE-2011-3026 and is fixed in version 1.5.9 (and versions 1.4.9, 1.2.47, and 1.0.57, respectively, on the older branches), released 18 February 2012.

Vulnerability Warning

libpng 1.5.4 through 1.5.7 contain a one-byte (stack) buffer-overrun bug in `png_formatted_warning()`, which could lead to crashes (denial of service) or, conceivably, execution of hostile code. This vulnerability has been assigned ID CVE-2011-3464 and is fixed in version 1.5.8, released 1 February 2012.

Vulnerability Warning

libpng 1.5.4 (only) introduced a divide-by-zero bug in `png_handle_cHRM()`, which could lead to crashes (denial of service) in applications that support color correction. This vulnerability has been assigned ID CVE-2011-3328 (CERT VU#477046) and is fixed in version 1.5.5, released 22 September 2011.

Vulnerability Warning

All released versions of libpng (from 1.0 onward) have a buffer overrun in the code that promotes palette images with transparency (1 channel) to grayscale+alpha images (2 channels), but only for applications that call `png_rgb_to_gray()` and not `png_set_expand()`. (None are known.) An arbitrary amount of memory may be overwritten in this case, with arbitrary (attacker-controlled) data. This vulnerability has been assigned ID CVE-2011-2690.

libpng 1.2.20 and later crashes in `png_default_error()` due to internal use of a NULL pointer instead of the empty string (""). This vulnerability has been assigned ID CVE-2011-2691.

Many (most?) versions of libpng read uninitialized memory when handling empty sCAL chunks, and they handle malformed sCAL chunks (those lacking a delimiting NULL between the internal strings) incorrectly. This vulnerability has been assigned ID CVE-2011-2692.

All of these issues are fixed in version 1.5.4 (as well as 1.4.8, 1.2.45, and 1.0.55 on the older branches), released 7 July 2011.

Vulnerability Warning

libpng 1.5.0 (only) introduced a bug in the RGB-to-grayscale transform code, which can lead to buffer overruns due to incorrect calculation of the number of bytes per pixel. (Since 1.5.0 was just released, no apps or OS distributions are believed to ship with it, so the risk should be minimal.) This vulnerability has been assigned ID CVE-2011-0408 (CERT VU#643140) and is fixed in version 1.5.1, released 3 February 2011.

Vulnerability Warning

Several versions of libpng through 1.4.2 (and through 1.2.43 in the older series) contain a bug whereby progressive applications such as web browsers (or the rpng2 demo app included in libpng) could receive an extra row of image data beyond the height reported in the header, potentially leading to an out-of-bounds write to memory (depending on how the application is written) and the possibility of execution of an attacker's code with the privileges of the libpng user (including remote compromise in the case of a libpng-based browser visiting a hostile web site). This vulnerability has been assigned ID CVE-2010-1205 (via Mozilla).

An additional memory-leak bug, involving images with malformed sCAL chunks, is also present; it could lead to an application crash (denial of service) when viewing such images.

Both bugs are fixed in versions 1.4.3 and 1.2.44, released 25 June 2010.

Vulnerability Warning

Jeff Phillips reported that several versions of libpng through 1.2.35 contain an uninitialized-memory-read bug that may have security implications. Specifically, 1-bit (2-color) interlaced images whose widths are not divisible by 8 may result in several uninitialized bits at the end of certain rows in certain interlace passes being returned to the user. An application that failed to mask these out-of-bounds pixels might display or process them, albeit presumably with benign results in most cases. This bug may be fixed in version 1.2.36, released 7 May 2009, but the correct fix is in version 1.2.37, released 4 June 2009.

Vulnerability Warning

All versions of libpng from 0.89c through 1.2.34 contain an uninitialized-data bug that can be triggered by a malicious user. Specifically, there are several instances in which a malloc'd array of pointers is then initialized by a secondary sequence of malloc() calls. If one of these calls fails, libpng's cleanup routine will attempt to free the entire array, including any uninitialized pointers, which could lead to execution of an attacker's code with the privileges of the libpng user (including remote compromise in the case of a libpng-based browser visiting a hostile web site). This vulnerability has been assigned ID CVE-2009-0040 and is fixed in version 1.2.35, released 18 February 2009.

Vulnerability Warning

Versions 1.2.30 and 1.2.31 of libpng can crash when reading images with multiple zTXt chunks; it is likely that this vulnerability could lead to a remote compromise in the case of a libpng-based browser visiting a hostile web site. This vulnerability has been assigned ID CVE-2008-3964 and is fixed in version 1.2.32, released 18 September 2008.

Vulnerability Warning

All versions of libpng from 1.0.6 through 1.2.26 have a bug when handling unknown (to libpng) chunks with zero data length. Applications that call either `png_set_read_user_chunk_fn()` or `png_set_keep_unknown_chunks()`, when used with standard builds of libpng (i.e., built with either PNG_READ_UNKNOWN_CHUNKS_SUPPORTED or PNG_READ_USER_CHUNKS_SUPPORTED defined), can crash when attempting to free a non-existent data buffer for the unknown chunk. The **pngtest** sample application distributed with libpng, **pngcrush**, and certain versions of **ImageMagick** are known to be affected, but the bug is otherwise believed to be quite rare. This vulnerability has been assigned ID CVE-2008-1382 and is fixed in version 1.2.27, released 28 April 2008.

Crash Warning

Most versions of libpng up through 1.2.24 have a number of minor coding errors that could lead to crashes in exceptional cases. For example, if memory allocation fails while processing certain ancillary chunks, libpng could crash while attempting to write to the NULL pointer; or if the application author failed to set up the `info_ptr` as required, some parts of libpng fail to check for NULL and could crash trying to read the pointer (though it's probable that the error would have caused libpng to terminate upstream of these parts). The bugs are fixed in version 1.2.25, released 18 February 2008.

Vulnerability Warning

Version 1.2.21 has a crash bug when reading the ICC-profile chunk, iCCP (CVE-2007-5267). This bug is fixed in version 1.2.22, released 13 October 2007.

Vulnerability Warning

Versions 1.2.20 and earlier have a number of potential crash-bugs due to out-of-bounds reads in certain chunk-handlers; MITRE has collectively assigned them the identifiers CVE-2007-5266, CVE-2007-5268 and CVE-2007-5269. These bugs are fixed in version 1.2.21, released 4 October 2007, but another crash bug (related to the ICC-profile chunk) remains to be fixed in version 1.2.22.

Vulnerability Warning

Versions up through 1.2.16 (and 1.0.24) have an NULL-pointer-dereference vulnerability involving palette images with a malformed tRNS chunk (i.e., one with a bad CRC value). This bug can, at a minimum, cause crashes in browsers simply by visiting a page displaying such an image; reportedly it also crashes the Microsoft Windows display manager. CERT refers to it as VU#684664 and MITRE as CVE-2007-2445. It's fixed in versions libpng 1.2.18 and libpng 1.0.26 (also 1.2.17 and 1.0.25, which had a bug in their configure scripts), released 15 May 2007.

Vulnerability Warning

Versions 1.0.6 through 1.2.12 and 1.0.20 have a bug in the decoder for the sPLT ("suggested palette") chunk; this can lead to crashes and, accordingly, a denial of service (e.g., crashing your browser when you visit a site displaying a specially crafted PNG). The bug is fixed in libpng 1.2.13 and libpng 1.0.21, released 15 November 2006. MITRE refers to this bug as CVE-2006-5793.

The same releases also include fixes for a specific class of application error (NULL png_ptr) and for a bug in the code that *writes* the iCCP ("ICC profile") chunk.

Vulnerability Warning

Versions up through 1.2.11 and 1.0.19 have a buffer-overrun vulnerability when a particular error message is triggered. The overrun is always by exactly two bytes ('k' and NULL) so it seems highly unlikely that it could be used for anything more nefarious than denial of service (e.g., crashing your browser when you visit a site displaying a specially crafted PNG). Nevertheless, it's worth fixing, and versions **libpng 1.2.12** and **libpng 1.0.20**, released 27 June 2006, do just that. (Note that 1.2.11 and 1.0.19 erroneously claimed to include the fix, but in fact it had been inadvertently omitted.) MITRE refers to this bug as CVE-2006-3334.

The same releases (and their immediate predecessors) also fix an out-of-bounds (by one) memory read and a second buffer overrun, this one in the code that *writes* the sCAL ("physical scale of subject") chunk (which is rather rare in any case).

There have been other issues in older versions released in 2004:

Crash Warning

Versions 1.2.7, 1.2.6, 1.0.17, and 1.0.16 have a bug that will cause applications that strip the alpha channel (while reading a PNG) to crash. The bug is fixed in versions **1.2.8** and **1.0.18**, which were released on 3 December 2004. MITRE refers to this bug as CVE-2006-0481.

The release before that fixed another bug, this one in the PNG-writing code:

Broken-Image Warning

Versions 1.2.6 and 1.0.16 can write an invalid zlib header within the PNG datastream. This is not quite as bad as it sounds since the two-byte header can be corrected fairly easily (e.g., use pngcrush to rewrite the images and, perhaps, compress them slightly better, or run the *png-fix-IDAT-windowsize* utility bundled with pngcheck 2.1.0 or later), but some applications will display the images incorrectly. Microsoft Word and Internet Explorer are known to be affected. A libpng patch is available, and versions **1.2.7** and **1.0.17** (incorporating the fix) were released on 11 September 2004.

Finally--and most important--there were several security vulnerabilities present in versions of libpng prior to 1.2.6 and 1.0.16, one of which is quite dangerous:

Vulnerability Warning

On 4 August 2004 a new **jumbo security patch** was released to address several potential vulnerabilities in libpng, at least one of which is *quite serious*. It was followed on 15 August by the full **libpng 1.2.6** and **libpng 1.0.16** releases, which, like subsequent releases, incorporate the fix. All users are strongly urged to upgrade to the latest release of libpng or to patch any affected applications as soon as possible. *(Graphical browsers and e-mail*

clients are particularly at risk.) Get the latest releases or an appropriate combo patch either from SourceForge (headings 1.2.5-security-patches and 1.2.5and-older-sec-patchs) or from Simple Systems.

Here's the CERT advisory, along with the relevant CERT and MITRE vulnerability pages:

- CERT VU#388984 (CVE CAN-2004-0597) (this is the serious one!)
- CERT VU#160448 (CVE CAN-2004-0599)
- CERT VU#236656 (CVE CAN-2004-0598)
- CERT VU#286464 (CVE CAN-2004-0599)
- CERT VU#477512 (CVE CAN-2004-0599)
- CERT VU#817368 (CVE CAN-2004-0597)

These vulnerabilities were discovered by Chris Evans and are also described in his alert. (Many thanks to Chris for notifying the libpng team and for providing time to fix the bugs before the public announcement!)

- PNG Home Page
- Complete PNG Site Map

Last modified 15 November 2015. Please direct libpng comments and questions to the png-mng-implement mailing list.

Web page copyright © 2000-2015 Greg Roelofs. libpng copyright 1995-2015 contributing authors.