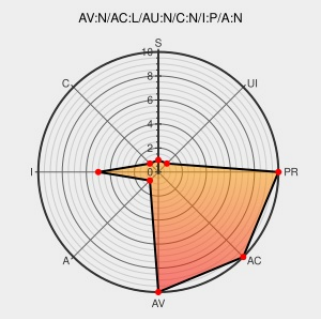
CVE-2008-5907

Published on: 01/15/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:16 PM UTC

CVE-2008-5907

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

The png_check_keyword function in pngwutil.c in libpng before 1.0.42, and 1.2.x before 1.2.34, might allow context-dependent attackers to set the value of an arbitrary memory location to zero via vectors involving creation of crafted PNG files with keywords, related to an implicit cast of the '\0' character constant to a NULL pointer. NOTE: some sources incorrectly report this as a double free vulnerability.

CVE-2008-5907 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - libpng non issue	Mailing List, Third Party Advisory, openwall.com, text/html	MLIST [oss-security] 20090109 libpng non issue
Gentoo update for libpng - Advisories - Community	Third Party Advisory, web.archive.org, text/html	SECUNIA 34320
Gentoo Linux Documentation -- libpng: Multiple vulnerabilities	Third Party Advisory, security.gentoo.org, text/html	GENTOO GLSA-200903-28
IBM X-Force Exchange	Third Party Advisory	XF libpng-pngcheckkeyword-

	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	memory-corruption(48128)
PNG and MNG/JNG image formats: home site / Thread: [png-mng-implement] Memory overwriting bug in png_check_keyword()	Third Party Advisory sourceforge.net text/html	MLIST [png-mng-implement] 20081126 Memory overwriting bug in png_check_keyword()
LIBPNG	Third Party Advisory libpng.sourceforge.net text/html	CONFIRM libpng.sourceforge.net/index.html
Debian update for libpng - Secunia Advisories - Vulnerability Information - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 34388
Advisories | Mandriva	Third Party Advisory www.mandriva.com text/html	MANDRIVA MDVSA-2009:051
Debian -- Security Information -- DSA-1750-1 libpng	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-1750
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:003	Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SR:2009:003

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Application	Libpng	Libpng	All	All	All	All
Application	Libpng	Libpng	All	All	All	All

cpe:2.3:o:debian:debian_linux:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*

cpe:2.3:a:libpng:libpng:*:*:*:*:*:*:*:*

cpe:2.3:a:libpng:libpng:*:*:*:*:*:*:*:*

← Previous ID

Next ID→