The buffer overflow could in a worst case scenario be used to execute arbitrary code. Libpng is used by important applications like the Mozilla Suite.

US-Cert yesterday announced Technical Cyber Security Alert TA04-217A. "Several vulnerabilities exist in the libpng library, the most serious of which could allow a remote attacker to execute arbitrary code on an affected system."

The alert addresses four security issues:

- **CAN-2004-0597** - Multiple buffer overflows exist, including when handling transparency chunk data, which could be exploited to cause arbitrary code to be executed when a specially crafted PNG image is processed
- **CAN-2004-0598** - Multiple NULL pointer dereferences in png_handle_iCPP() and elsewhere could be exploited to cause an application to crash when a specially crafted PNG image is processed
- **CAN-2004-0599** - Multiple integer overflows in png_handle_sPLT(), png_read_png() actions and elsewhere could be exploited to cause an application to crash, or potentially arbitrary code to be executed, when a specially crafted PNG image is processed
- **CAN-2004-0768** - A buffer overflow could be caused by incorrect calculation of buffer offsets, possibly leading to the execution of arbitrary code

SuSE Linux announced updated libpng packages yesterday, followed by Gentoo Linux and Trustix Linux who made patched versions of libpng available today.

- Suse Linux made safe libpng packages available 2004-08-14.
  - The full SUSE Security Announcement SUSE SA_2004_023
- Gentoo Linux made safe libpng packages available 2004-08-15 (emerge sync && emerge libpng)
  - libpng-1.2.5-r8 package details
  - libpng: Numerous vulnerabilities
- Trustix Linux made safe libpng packages available 2004-08-15.
  - Trustix Secure Linux Security Advisory #2004-0040
- Check your distributions homepage and/or bugzilla to find your distributions libpng status.

Libpng 1.2.6rc1 is safe and is available from the libpng sourceforge project page. Libpng 1.2.6 will be released sometime this month.