netpbm

The netpbm package contains a library of functions that support programs for handling various graphics file formats, including .pbm (portable bitmaps), .pgm (portable graymaps), .pnm (portable anymaps), .ppm (portable pixmaps) and others.

A bug was found in the way netpbm converts Portable Anymap (PNM) files into Portable Network Graphics (PNG). This problem with netpbm creates a situation where the use of uninitialized variables in the pnmtopng code allows an attacker to change stack contents when converting to PNG files with pnmtopng using the *-trans* option.

This situation may allow an attacker to execute arbitrary code. The Common Vulnerabilities and Exposures project assigned the name CAN-2005-2978 to this issue.

Debian reference: DSA-878-1
Gentoo reference: GLSA 200510-18
Red Hat reference: RHSA-2005:793-6
Suse reference: SUSE-SR:2005:02

Lynx

Lynx is a text-based web browser.

Ulf Harnhammar discovered a stack overflow bug in the way Lynx handles connections to NNTP (news) servers. An attacker could create a web page redirecting to a malicious news server that could execute arbitrary code as the user running lynx. The Common Vulnerabilities and Exposures project assigned the name CAN-2005-3120 to this issue.

Debian reference: DSA-876-1
Gentoo reference: GLSA 200510-15
Mandriva reference: MDKSA-2005:186
Red Hat reference: RHSA-2005:803-4
Suse reference: SUSE-SR:2005:02

Ruby

Ruby is an interpreted scripting language for object-oriented programming.

A bug was found in the way Ruby handles eval statements. It is possible for an attacker to exploit this bug by creating a malicious script that could call eval in a way that would have the effect of letting the system bypass certain safe-level restrictions. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-2337 to this issue.

Debian reference: DSA-864-1
Mandriva reference: MDKSA-2005:191
Red Hat reference: RHSA-2005:799-6

Sudo

Sudo (Superuser Do) is a program for Linux and Unix-based systems that lets an ordinary user execute commands as superuser.

Tavis Ormandy discovered that sudo does not perform sufficient environment cleaning; in particular, the SHELLOPTS and PS4 variables are still passed to the program running as an alternate user, which can result in the execution of arbitrary commands as the alternate user when a bash script is executed. The Common Vulnerabilities and Exposures project assigned the name CVE-2005-2959 to this issue.

Debian reference: DSA-870-1
Mandriva reference: MDKSA-2005:201