PHP

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Web server.

A bug was discovered in the PEAR XML-RPC Server package included in PHP. If a PHP script is used that implements an XML-RPC Server using the PEAR XML-RPC package, it is possible for a remote attacker to construct an XML-RPC request that can cause PHP to execute arbitrary PHP commands as the 'apache' user. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-1921 to this issue.

A race condition in temporary file handling was discovered in the shtool script installed by PHP. If a third-party PHP module that uses shtool is compiled as root, a local user may be able to modify arbitrary files. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-1751 to this issue.

Users of PHP should upgrade to the updated packages, which contain backported fixes for these issues.

Gentoo reference: GLSA 200507-08
Mandriva reference: MDKSA-2005:109
Red Hat reference: RHSA-2005:564-15
Suse reference: SUSE-SA:2005:041

REALPLAYER

RealPlayer is a media player that provides media playback locally and via streaming. It plays RealAudio, RealVideo, MP3, 3GPP Video, Flash, SMIL 2.0, JPEG, GIF, PNG, and more.

A buffer overflow bug was found in the way RealPlayer processes SMIL files. An attacker could create a specially crafted SMIL file that could combine with a malicious Web server to execute arbitrary code when the file was opened by a user. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-1766 to this issue.

Gentoo reference: GLSA 200507-04
Red Hat reference: RHSA-2005:523-09
Suse reference: SUSE-SA:2005:037

SUDO

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root with logging.

A race condition bug was found in the way sudo handles pathnames. It is possible that a local user with limited sudo access could create a race condition that would allow the execution of arbitrary commands as the root user. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-1993 to this issue.

Debian reference: DSA-735-1
Gentoo reference: GLSA 200506-22
Mandriva reference: MDKSA-2005:103
Red Hat reference: RHSA-2005:535-06
Slackware reference: SSA:2005-172-01
Suse reference: SUSE-SA:2005:036