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 with the PHP scripting language.

If a user tries to execute a PHP script that implements an XML-RPC Server using the PEAR XML-RPC package, it is possible that a malicious remote attacker could construct an XML-RPC request which could cause PHP to execute arbitrary PHP commands as the Apache user.

The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-2498 to this problem with the PEAR XML-RPC Server package.

Debian reference: DSA-789-1 php4
Gentoo reference: GLSA 200507-01
Mandriva reference: MDKSA-2005:146
Red Hat reference: RHSA-2005:748-05
Slackware reference: SSA:2005-251-04
Suse reference: SUSE-SA:2005:049

Evolution

Evolution is the GNOME collection of personal information management (PIM) tools. A format string bug was found in Evolution. If a user tries to save a carefully crafted meeting or appointment, arbitrary code may be executed as the user running Evolution. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-2550 to this issue.

Additionally, several other format string bugs were found in Evolution. If a user views a malicious vCard, connects to a malicious LDAP server, or displays a task list from a malicious remote server, arbitrary code may be executed as the user running Evolution. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-2549 to this issue.

Gentoo reference: GLSA 200508-12 / evolution
Mandriva reference: MDKSA-2005:141
Red Hat reference: RHSA-2005:267-10

PCRE

PCRE is a Perl-compatible regular expression library.

An integer overflow flaw was found in PCRE. On systems that accept arbitrary regular expressions from untrusted users, this flaw could be exploited to execute arbitrary code with the privileges of the application using the library. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-2491 to this issue.

The security impact of this issue varies depending on the way the application uses PCRE. For example, the Apache Web server uses the system PCRE library in order to parse regular expressions, but this flaw would only allow a user who already has the ability to write .htaccess files to gain apache privileges.

Debian reference: DSA-800-1 pcre3
Mandriva reference: MDKSA-2005:151
Red Hat reference: RHSA-2005:761-5
Slackware reference: SSA:2005-242-01
Suse reference: SUSE-SA:2005:048