method are not affected. Python users should upgrade to the latest version.
GLSA 200502-09 / Python
MDKSA-2005:017

SQUID

Squid is a full-featured Web proxy cache designed to run on Unix systems. It supports proxying and caching of HTTP, FTP, and other protocols, as well as SSL support, cache hierarchies, transparent caching, access control lists and many other features.

Squid contains several vulnerabilities: Buffer overflow when handling WCCP recvfrom() (CAN-2005-0211). Loose checking of HTTP headers (CAN-2005-0173 and CAN-2005-0174). Incorrect handling of LDAP login names with spaces (CAN-2005-0175).

An attacker could exploit:

- the WCCP buffer overflow to cause Denial of Service.
- the HTTP header parsing vulnerabilities to inject arbitrary response data, potentially leading to content spoofing, web cache poisoning and other cross-site scripting or HTTP response splitting attacks.
- the LDAP issue to log in with several variations of the same login name, leading to log poisoning.

All Squid users should upgrade to the latest version.
DSA-667-1 squid
GLSA 200502-04 / squid
SUSE-SR:2005:003

PERL

Perl is a high-level programming language commonly used for system administration utilities and Web programming.

Kevin Finisterre discovered a stack based buffer overflow flaw in sperl, the Perl setuid wrapper. A local user could create a sperl executable script with a carefully created path name, overflowing the buffer and leading to root privilege escalation. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0156 to this issue.

Kevin Finisterre discovered a flaw in sperl that allows debugging information to be logged to arbitrary files. By setting an environment variable, a local user could cause sperl to create, as root, files with arbitrary filenames, or append the debugging information to existing files. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-0155 to this issue.

The Debian Security Audit Project discovered that Perl's DBI library creates a temporary PID file in an insecure manner. A local user could overwrite or create files as a different user who happens to run an application using DBI::ProxyServer. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-0077 to this issue.
MDKSA:2005:030 perl-DBI
MDKSA:2005:031 perl
RHSA-2005:069-08
RHSA-2005:105-11