## GAIM

Gaim is an Internet Messaging client. A heap-based buffer overflow issue was discovered in the way Gaim processes away messages. A remote attacker could send a specially crafted away message to a Gaim user logged into AIM or ICQ that could result in arbitrary code execution. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-2103 to this issue.

Daniel Atallah discovered a denial of service issue in Gaim. A remote attacker could attempt to upload a file with a specially crafted name to a user logged into AIM or ICQ, causing Gaim to crash. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-2102 to this issue. A denial of service bug was found in Gaim's Gadu Gadu protocol handler. A remote attacker could send a specially crafted message to a Gaim user logged into Gadu Gadu, causing Gaim to crash. Please note that this issue only affects PPC and IBM S/390 systems running Gaim. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-2370 to this issue.

*Debian reference: DSA-769-1*
*Gentoo reference: GLSA 200508-06*
*Red Hat reference: RHSA-2005:627-11*
*Suse reference: SUSE-SR:2005:017*

## CUPS

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX and Linux operating systems. When processing a PDF file, bounds checking was not correctly performed on some fields. This could cause the pdftops filter (running as user "lp") to crash. The Common Vulnerabilities and Exposures project has assigned the name CAN-2005-2097 to this issue. All users of CUPS should install a patch to correct this issue.

*Mandriva reference: MDKSA-2005:138*
*Red Hat reference: RHSA-2005:706-04*

## FETCHMAIL

Fetchmail is a remote mail retrieval and forwarding utility. The fetchmail mail program retrieves mail from servers and forwards it via SMTP, so that it can be read by mail user agents such as mutt and elm.

A buffer overflow was discovered in fetchmail's POP3 client. It is possible that a malicious server could send a carefully crafted message UID and cause fetchmail to crash or potentially execute arbitrary code as the user running fetchmail.

The Common Vulnerabilities and Exposures project assigned the name CAN-2005-2335 to this issue. Users of fetchmail should update to the latest package, which contains a backported patch to correct this issue.

*Debian reference: DSA-774-1*
*Gentoo reference: GLSA 200507-21*
*Red Hat reference: RHSA-2005:640-08*
*Slackware reference: SSA:2005-203-05*
*Suse reference: SUSE-SR:2005:018*