

CVS Trouble

Contributed by Duke

Welcome to Security Alerts, an overview of recent Unix and open source security advisories. In this column, we look at problems in CVS, PostgreSQL, Squid, Gaim, Debian's lsh, Xine-lib, Caroline, Convert-UUlib, Rootkit Hunter, snmppd, Kommander, kimgio, RealPlayer, Helix Player, xli, and Debian's samba.

* CVS * PostgreSQL * Squid * Gaim * Debian's lsh * Xine-lib * Caroline * Convert-UUlib * Rootkit Hunter * snmppd * Kommander * kimgio * RealPlayer and Helix Player * xli * Debian's samba
 CVS (Concurrent Versions System) is a popular open source, source-code version-management system. Under certain conditions, the pserver access method can be bypassed to gain unauthorized access to the repository without using the password. Also under some conditions involving the cvs-repouids file, CVS can be vulnerable to a denial-of-service-based attack. It is recommended that users upgrade to version 1.11.20 or newer of CVS and consider disabling the pserver authentication method until it has been upgraded.

PostgreSQL Multiple buffer overflows have been reported in the PostgreSQL parser. These may be exploitable by an attacker to execute arbitrary code with the permissions of the user account running the database. Users should watch their vendors for a repaired version of PostgreSQL.

Squid The open source, web proxy cache server Squid is reported to have two security-related problems that could, under some conditions, be exploited by a remote attacker to gain unexpected permissions or view cookies from other users. Affected users should upgrade to Squid 2.5.STABLE9 or newer as soon as possible.

Gaim Gaim is a Linux, BSD, Mac OS X, and Windows instant messaging client that supports AIM, ICQ (Oscar protocol), MSN Messenger, Yahoo!, IRC, Jabber, Gadu-Gadu, SILC, GroupWise Messenger, and Zephyr networks. Remotely exploitable denial-of-service vulnerabilities have been reported in Gaim. The vulnerabilities are located in the gaim_markup_strip_html() function, the IRC protocol plugin, and in code dealing with file transfers for Gaim Jabber users. Users of Gaim should upgrade to version 1.2.1 or newer.

Debian's lsh lsh, the GNU implementation of OpenSSH or SSH, is reported to have a buffer overflow and a denial-of-service vulnerability in old versions of the lshd daemon. The buffer overflow may be exploitable by a remote attacker to execute arbitrary code with root permissions. Debian has released updated versions of lsh to repair these vulnerabilities. The buffer overflow does not seem to be a new problem; users who have a lshd earlier than 1.4.3 should consider upgrading.

Xine-lib Xine-lib, a multimedia video library used by the free Linux media player Xine, is reported to be vulnerable to buffer overflows in code that handles RealMedia RTSP (Real Time Streaming Protocol) and MMST (Microsoft Media Services streams over TCP). Successfully exploiting these buffer overflows could result in arbitrary code being executed on the victim's machine. The Xine developers strongly encourage users to upgrade to version 1.0.1 as soon as possible.

Caroline Caroline, an open source collaborative learning environment written with PHP and MySQL that allows teachers and education institutions to create and administer web-based courses, is vulnerable to multiple remote attacks. These vulnerabilities could be exploited under some conditions by a remote attacker to execute arbitrary code with the permissions of the user running the web server, make unauthorized changes to the database, cause code to be executed in other users' web browsers, or to gather unauthorized information about the server's file system. All users of Caroline are strongly encouraged to upgrade to version 1.54 or 1.6 final.

Convert-UUlib Convert-UUlib provides a Perl interface to the uuilib library. A buffer overflow in Convert-UUlib may be exploitable by an attacker to execute arbitrary code with the victim's permissions. Users should upgrade to Convert-UUlib version 1.051.

Rootkit Hunter Rootkit Hunter, a security testing tool, is reported to be vulnerable to an attack based on a temporary-file, symbolic-link race condition. This may be exploitable to overwrite arbitrary files on the system with the permissions of the user running Rootkit Hunter. Affected users should upgrade to Rootkit Hunter version 1.2.3-r1 or newer as soon as possible.

snmppd snmppd is a SNMP proxy daemon designed to work with the monitoring tool Nagios. snmppd is vulnerable to a format-string bug that may be exploitable to execute arbitrary code with root permissions. Users should watch for a repaired version of snmppd and should consider disabling it until it has been fixed.

Kommander Kommander, a graphical scripting tool for KDE that is distributed as part of the kdwebdev package, will run scripts from untrusted remote sources without requiring any user confirmation. Affected users should watch their vendors for updated kdwebdev packages.

kimgio kimgio is a KDE image handler distributed with the kdelib package. kimgio is vulnerable to a buffer overflow in code that loads PCX files. Exploiting this buffer overflow could result in arbitrary code being executed with the permissions of the user running KDE. Patches are available for KDE 3.4.0 and 3.3.2. Also in Security Alerts: [PHP Problems](#) [Ethereal Trouble](#) [KWord Trouble](#) [XFree86 Trouble](#) [MySQL Trouble](#)

RealPlayer and Helix Player RealPlayer and Helix Player are multimedia players from Real Networks. It is reported that both RealPlayer and Helix Player are vulnerable to buffer overflows when processing .ram files. Exploiting this vulnerability may result in arbitrary code being executed with the permissions of the user running RealPlayer or Helix Player. It is recommended that all users of RealPlayer or Helix Player upgrade to the latest available versions. Updates and more information is available from the RealNetworks security updates page.

xli xli, an X11 utility to load and view images, is vulnerable to a metacharacter-based attack when viewing a compressed image, and is also vulnerable to several buffer overflows. Users should upgrade to version 1.17 or should watch their vendors for a repaired version.

Debian's samba Debian has released updated samba packages that repair remotely exploitable buffer overflows. Affected users should upgrade as soon as possible.