

Buffer Overflows in SSH and PHP

Contributed by jhon

Welcome to Security Alerts, an overview of recent Unix and open source security advisories.

In this column, we look at buffer overflows in SSH, PHP, typespeed, Cyrus IMAP Server, Cyrus SASL library, and pdftops; and problems with PFinger, KDE, and zkfingerd.

- * SSH
- * PHP
- * PFinger
- * KDE
- * typespeed
- * The Cyrus IMAP Server
- * Cyrus SASL library
- * Common Unix Printing System pdftops
- * zkfingerd

SSH

Some SSH clients and servers have buffer overflows in the key exchange initialization and startup code that may be exploitable by a remote attacker in a denial-of-service attack or, under some conditions, allow the execution of arbitrary code as the root user. These buffer overflows are in code that is executed prior to user authentication.

Implementations of SSH that have been reported to be vulnerable by at least one source include: F-Secure Corp's SSH servers and clients for Unix (v3.1.0 build 11 and older) and Windows (v5.2 and older); SSH Communications Security, Inc. SSH for Unix and Windows (v3.2.2 and older); FiSSH SSH client for Windows (v1.0A and older); SecureNetTerm client for Windows (v5.4.1 and older) NetComposite ShellGuard SSH client for Windows (v3.4.6 and older); Pragma Systems, Inc. SecureShell SSH server for Windows (v2 and older); PuTTY SSH client for Windows (v0.53 and older); and WinSCP SCP client for Windows (v2.0.0 and older). A trojan SSH server has been released that exploits this problem in the PuTTY SSH client.

Some vendors that have been reported to be vulnerable are reporting that their software is not exploitable. It is recommended that users contact their vendor for information on their implementation of SSH. Users should also consider using a firewall to restrict the hosts that can connect to their machines. The risk to a vulnerable SSH client can be reduced by connecting to trusted hosts by IP address.

PHP

PHP's wordwrap() function has a buffer overflow that may be exploitable to execute arbitrary code with the permissions of the user running the script. The buffer overflow is reported to affect versions of PHP between 4.1.2 and 4.3.0. Scripts that do not contain the wordwrap() function call are not affected by this buffer overflow.

Affected users should upgrade to version 4.3.0 of PHP.

PFinger

PFinger, an open source alternative for the GNU Finger daemon, is vulnerable to a format-string vulnerability that can be exploited by a remote attacker to execute arbitrary code with the permissions of the user running the daemon. Exploiting this vulnerability requires that the attacker control or spoof the DNS server response to a query on a host that made a finger request.

Users should upgrade to PFinger version 0.7.9 as soon as possible. Users whose system do not use the service supplied by PFinger should consider disabling it.

KDE

KDE does not always properly quote the parameters passed to a shell for execution. This problem can be used, under some circumstances, by a remote attacker to execute commands on a machine with the permissions of the user running KDE. The parameters can be passed to the user through sources such as Web pages, email, or files.

The KDE Security Team strongly recommends that KDE 3.x users upgrade to KDE 3.0.5a, and states that KDE 2 users have been provided a patch against the KDE 2.2.2 source code that also repairs these problems. Users of operating system vendor supplied KDE packages should watch their vendor for updated packages.

typespeed

The typing speed game typespeed is vulnerable to a buffer overflow that can be used by a local attacker, under some conditions, to execute code with the group ID permissions of the group games.

Affected users should remove the games group ID until typespeed has been repaired. Debian has released repaired packages.

The Cyrus IMAP Server

The Cyrus IMAP Server, an open source application that provides Internet Message Access Protocol (IMAP) services, has a buffer overflow that can be exploited prior to login to execute arbitrary code or to read other users' email. This buffer overflow is present in versions of Cyrus IMAP earlier than 2.1.10 and 2.0.16.

It is recommended that affected users upgrade to versions 2.0.17 or 2.1.11 of Cyrus IMAP as soon as possible.

Cyrus SASL library

Buffer overflows found in the Cyrus SASL (Simple Authentication and Security Layer) library can, under some limited conditions, be exploited to execute arbitrary code on the system with the permissions of the user running the linked application.

Affected users should watch their vendor for an update to the Cyrus SASL library.

Common Unix Printing System pdftops

The print filter pdftops that is supplied with the Common Unix Printing System (CUPS) and with Xpdf has an integer overflow that can be exploited to execute arbitrary code. This code will be executed with the permissions of the user running lp or as the lp user, if it is installed set user id. The print filter pdftops converts a PDF file into a PostScript file.

CUPS version 1.1.18 is reported to contain a repaired version of pdftops and a patch has been released that can be applied to Xpdf version 2.01.

zkfingerd

zkfingerd is an open source Finger daemon. It is vulnerable to several format string vulnerabilities that can be exploited by a remote attacker to execute arbitrary commands with the permissions of the user running the daemon. A script to automate this vulnerability has been released.

Users of zkfingerd should upgrade using patches from its CVS repository. If finger is not being used on the system, zkfingerd should be disabled or removed.