

SAMBA Remote Root Exploit

Contributed by Aman

Welcome to Security Alerts, an overview of recent Unix and open-source security advisories. In this column, we look at buffer overflows in the GazTek HTTP Daemon, Solaris Printer Daemon, and w3m; a problem in default SAMBA installations that can be used to gain root access; and problems in Cisco 6400 NRP2, uirectory, Tarantella, Oracle 8i SQLNet, Formmail.pl, OS X directory permissions, and kdesu.

Samba

The Samba SMB file-sharing daemon `smbd` unsafely verifies its parameters and, on many systems, has an unsafe default configuration. Incoming NetBIOS computer names are not validated sufficiently and, in combination with the default configuration, can be exploited by a remote attacker to create SMB session log files in locations outside of the log directory. By using these flaws and a local account an attacker can gain root privileges. Any configuration of Samba that does not require a log prefix or suffix is vulnerable to a remote root compromise.

It is recommended that users of Samba turn off logging until a patch has been applied to fix these flaws.

Cisco 6400 NRP2

The Cisco 6400 NRP2 (Access Concentrator Node Route Processor 2) module will allow telnet connections to any of the 32 vtys, even if a password has not been set. The expected behavior is to deny telnet access when a password has not been set for the vtys.

Cisco recommends that users upgrade to IOS release 12.1(05)DC01 or newer. A workaround is to set a password for each of the 32 vtys.

GazTek HTTP Daemon

GazTek HTTP Daemon, a small HTTP server, has a buffer overflow that can be exploited by a remote attacker to execute arbitrary code with the permissions of the user running GazTek. An exploit script has been released.

Users should disable GazTek until a patched version has been installed.

uirectory

uirectory is a Web-based directory and listing system. During the opening of the category file, it passes a variable from the user to an `open()` system call without parsing it for shell meta-characters. Not filtering for meta-characters can be exploited by any remote user to execute arbitrary commands on the server as the user running uirectory.

Users should disable uirectory until a patch for this bug has been applied.

SCO Tarantella

Versions 3.00 and 3.01 of Tarantella have a bug in the `ttawebtop.cgi` program that can be used to read files on the system with the permissions of the user account running the webserver.

It is recommended that users upgrade to Tarantella version 3.10 as soon as possible.

Solaris Printer Daemon

The Solaris Printer Daemon, `in.lpd`, has a buffer overflow that can be used by a remote attacker to execute arbitrary code with the permissions of the root user, or used to crash the daemon. This vulnerability is reported to affect Solaris versions 2.6, 7, and 8.

Users should disable `in.lpd` until a patch from Sun has been installed.

Oracle 8i SQLNet

The implementation of the Transparent Network Substrate (TNS) over SQLNet that is used by Oracle 8i can be used in a denial-of-service attack against any of the Oracle services that are relying on TNS. Versions reported to be vulnerable include: Oracle 8i Standard and Enterprise Editions for Linux, Solaris, AIX, Windows, HP-UX, and Tru64 Unix with versions before 8.1.6.

It has been reported that Oracle has released a patch to solve this problem under bug number 1656431 but other sources have reported that they were unable to locate this patch. Users who are unable to locate this patch should contact Oracle for assistance.

Formmail.pl

Formmail.pl is a popular CGI program used to send email from a web form. A flaw in Formmail.pl can be exploited by a

spammer or other attacker to send anonymous email.

A new version has been released that fixes this flaw and provides protections against abuse.
OS X Directory Permissions

It has been reported that under some conditions under OS X, a user's Desktop directory is set with world-readable and -writable permissions.

The reports have been contradictory as to which versions, and under what conditions, the problem with the directory permissions occur. It is recommended that all users check the permissions of the Desktop directories on their system.
kdesu

The kdesu program that is part of the kdelibs package has a race condition that may be exploited to gain access to the X server, and may lead to a compromise of any accounts accessed via kdesu. When kdesu was used to su to an account, it would create a world-readable temporary file to exchange authentication information and then remove it.

It is recommended that users upgrade to the latest kdelib packages as soon as possible.

Solaris Buffer Overflows

Buffer overflows were reported in two optional Solaris packages and a library. The buffer overflows are in /opt/SUNWssp/bin/cb_reset, /opt/SUNWvts/bin/ptexec, and in the LDAP library libslldap under Solaris 8. The programs are installed set user id root, and the library is linked by many set user id root commands. These vulnerabilities can all lead to a root compromise.

Both of the programs should have their set user id bits removed until a patch from Sun has been installed, and the library should be patched as soon as a patch becomes available from Sun.

w3m

w3m is a console Web browser comparable to Lynx. It has a buffer overflow in the routine that parses MIME headers that can be exploited when the user downloads a carefully-crafted Web page to execute arbitrary code with the permissions of the user executing w3m.

Users of w3m should install a patched version as soon as possible