Insecurity News

Security flaw hits Windows, Mac, Linux

Systems that use Sun Microsystem's XDR software are vulnerable. This applies to MS Windows, Apple Mac OS X and Unix based systems. It is possible to gain root access and so take control of your system. The XDR library is available and used across a range of operating systems, so the flaw is not limited to any one OS in particular and even extends to Kerberos authentication systems.

The problem is widespread because it affects some implementations of XDR (external data representation) libraries, used by many applications as a way of sending data from one system process to another, regardless of the computer system's architecture.

The affected libraries are all derived from Sun Microsystem's SunRPC remote procedure call technology, which has been taken up by many vendors. The Computer Emergency Response Team (CERT), a security network based at Carnegie Mellon University, warned that systems using the affected code should immediately apply patches or disable the affected services.

Cory Cohen and Jeffrey Havrilla from CERT report that the integer overflow in the library can lead to buffer overflows these in turn can allow unauthorised users to compromise the system by either executing other program code, taking data or taking down a system. With the Kerberos 5 administration system an unauthorised user could take control the Key Distribution Center authentication functions. The Kerberos development team at MIT has issued a warning and patch on their website. Patches are also available from CERT, Apple or the Linux distributors' websites. ■

Trojan OpenSSH

CERT Advisory CA-2002-24 CERT has received confirmation that some copies of the source code for the OpenSSH package have been modified by an intruder and contain a Trojan horse. The following three files were modified to include the malicious code: openssh-3.4p1.tar.gz openssh-3.4.tgz openssh-3.2.2p1.tar.gz .

These files appear to have been placed on the FTP server which hosts ftp.openssh.com and ftp.openbsd.org on the 30th or 31st of July, 2002. The OpenSSH development team replaced the Trojan horse copies with the original, uncompromised versions at 13:00 UTC, August 1st, 2002. The Trojan horse copy of the source code was available long enough for copies to propagate to sites that mirror the OpenSSH site.

The Trojan horse versions of OpenSSH contain malicious code that is run when the software is compiled. This code is used to connect to a fixed remote server on port 6667/tcp. It can then be used to open a shell running as the user who compiled OpenSSH. ■

Red Hat

Util-Linux

The Red Hat Network site at *rhn.redhat.com/errata/RHSA-2002-132.html* reports a vulnerability in the util-linux package. This security error was discovered by the BindView RAZOR Team. By exploiting the flaw it is possible to allow a local user to use privilege escalation when the ptmptmp file is not removed properly when using the chfn utility.

The util-linux package contains a host of utilities such as fstab, mkfs, and chfn. Because setpwnam.c inadequately locks a temporary file that is used when it is making changes to */etc/passwd*, a race condition could be used by the exploiter to elevate his privileges on the system, and so compromise security. This new vulnerability is not limited to the Red Hat distribution alone.

PHP errors

A vulnerability has been discovered in PHP versions 4.2.0 and 4.2.1. It is feared that this vulnerability could be used by a remote attacker to execute arbitrary code or crash PHP and/or the web server. The vulnerability occurs inside the portion of PHP code, which is responsible for the handling of the file uploads, specifically multipart and form-data. However, by sending a specially crafted POST request to the web server, an attacker could now corrupt the internal data structures used by PHP. In this way an intruder could cause an improperly initialized memory structure to be freed.

In most cases, an intruder could then use this flaw to crash PHP or the web server. Under some circumstances, an intruder then might be able to take advantage of this flaw and execute arbitrary code with the privileges of the web server.

This vulnerability was discovered by the e-matters GmbH team and this is described in great detail in their security advisory. Stefan Esser of e-matters GmbH has indicated that fortunately intruders cannot execute code on any x86 systems. The vulnerability is not limited to just the Red Hat distribution alone. ■

Mandrake

Apache

A Denial of Service attack was discovered by Mark Litchfield in the Apache webserver. While they were investigating this common problem, the Apache Software Foundation also discovered that the code for handling invalid requests that uses chunked encoding might also allow some arbitrary code to be executed on 64bit architectures. All versions of Apache prior to 1.3.26 and 2.0.37 are vulnerable to this problem.

Msec

The Mandrake Linux Security tool usually called msec has a potential security vulnerability. The msec utility will restore the default property settings during a periodic system audit. These default settings being 755 mode for each user's home directory. CERT/CC does not believe that this utility represents any security vulnerability as this behaviour is accurate and maintains the configured security policy. This is consistent with the product documentation. ■

Debian

dietlibc

The RPC library which is used by the dietlibc package, being a size optimized libc, has had an integer overflow error discovered. The RPC code is derived from the SunRPC library. By exploiting this security flaw it is possible to gain root access to any software which is linked to this library code.

These problems have now been fixed in version 0.12-2.2 for the current stable Debian distribution (woody) and also in the version 0.20-0cvs20020806 for the unstable distribution (sid). Debian GNU/Linux 2.2 (potato) is not affected since it does not contain the dietlibc packages. The vulnerability is not limited to the Debian GNU/Linux distributions. It can occur in any system in which the package has been installed.

tinyproxy

A small bug has been found by the authors of tinyproxy, a small sized HTTP proxy program, in the way that it handles certain invalid proxy requests. It might be possible that in some cases the invalid proxy request may result in the freeing of an allocated memory block to happen twice. This in turn could then lead to the execution of arbitrary code.

This problem has been fixed in version 1.4.3-2woody2 for the current stable distribution (woody) and in version 1.4.3-3 for the unstable distribution (sid). The old stable distribution (potato) is not affected by this problem. This security vulnerability is not limited to Debian GNU/Linux alone.

super

The super package which can be used to provide certain system users access to particular users and programs has been found to have a vulnerable use of format strings. By exploiting this bug a local user could possibly gain root access.

This problem has been fixed in version 3.12.2-2.1 for the old stable distribution (potato), in version 3.16.1-1.1 for the current stable distribution (woody) and in version 3.18.0-3 for the unstable distribution (sid). The vulnerability is not limited to Debian alone. ■

gallery

The gallery program, which is a web-based photo album toolkit, has had a vulnerability discovered. It is possible to remotely pass in the GALLERY_BASEDIR variable. By doing this, it is possible to execute commands and so compromise the system under the uid of the web server. This has been fixed in version 1.2.5-7 of the Debian package and upstream version 1.3.1. The vulnerability is not limited to Debian alone.

mm

Sebastian Krahmer and Marcus Meissner have both discovered, as well as fixed, a temporary file vulnerability in the mm shared memory library. This error could be exploited to gain root access onto a machine which is running Apache that is linked against this library and if shell access to the user "www-data" is already available (and this could be also triggered easily through PHP).

This problem has been fixed in the upstream version 1.2.0 of mm, which will be uploaded to the unstable Debian distribution while this advisory is released. Fixed packages for potato (Debian 2.2) and woody (Debian 3.0) are linked below. The vulnerability is not limited to Debian alone.

libapache-mod-ssl

The libapache-mod-ssl package provides SSL capability to the apache webserver. Recently, a problem has been found in the handling of .htaccess files, allowing arbitrary code execution as the web server user (regardless of ExecCGI / suexec settings), DoS attacks (killing off apache children), and allowing someone to take control of apache child processes – all through specially crafted *.htaccess* files.

More information about this security vulnerability can be found at *online.securityfocus.com/bid/5084*

This error has now been fixed for the libapache-mod-ssl_2.4.10-1.3.9-1potato2 package (for potato), and also in the libapache-mod-ssl_2.8.9-2 package (for woody). The vulnerability is not limited to Debian alone. ■

SuSE

wwwoffle

SuSE reference SuSE-SA:2002:029 The WWWOFFLE, World Wide Web Offline Explorer, program suite acts as a HTTP, FTP and Finger proxy to allow users with dial-up access to the internet to do offline WWW browsing. The parsing code of wwwoffled that processes HTTP PUT and POST requests fails to handle a Content Length value smaller then -1. It is believed that an attacker could exploit this bug to gain remote wwwrun access to the system wwwoffled is running on.

Temporarily, the wwwoffle daemon can be disabled in the following way (as root): *rcwwwoffle stop*.

bind, glibc

A vulnerability has been discovered in some resolver library functions. The affected code goes back to the resolver library shipped as part of BIND4; code derived from it has been included in later BIND releases as well as the GNU libc.

The bug itself is a buffer overflow that can be triggered if a DNS server sends multiple CNAME records in a DNS response.

This bug has been fixed for the gethostbyXXX class of functions in GNU libc in 1999. Unfortunately, there is similar code in the getnetbyXXX functions in recent glibc implementations, and the code is enabled by default, but, these functions are used by very few applications, such as ifconfig and ifuser, which makes exploits less likely.

Until glibc patches are available, you should disable DNS lookups of network names in nsswitch.conf. Simply replace the line containing the tag "networks:" with this line: networks: files. If having configured a name to network mapping via DNS, copy this information to /etc/networks.

The resolver bug is also in the libbind library included in BIND. This library is used by the bindutil package. ■

INFO

www.cert.org/
www.vulnwatch.org/
rhn.redhat.com/errata/
www.linux-mandrake.com/en/security/
www.suse.de/uk/support/security/index.html