Insecurity News

Apache/mod_ssl Worm

The Apache/mod_ssl worm scans for vulnerable systems on 80/tcp using an invalid HTTP GET request. GET /mod_ssl:error:HTTP-request HTTP/1.0. When an Apache system is detected, it attempts to send exploit code to the SSL service via 443/tcp. If successful, a copy of the malicious source code is then placed on the victim server, where the attacking system tries to compile and if sucessful, run it.

Once infected, the victim server begins scanning for additional hosts to continue the worm's propagation. The worm can act as an attack platform for distributed denial-of-service (DDoS) attacks against other sites by building a network of infected hosts.

During the infection process, the attacking host instructs the newly-infected victim to initiate traffic on 2002/udp back to the attacker. Once this communications channel has been established, the infected system becomes part of the Apache/mod_ssl worm's DDoS network. Hosts can then share information on other infected systems as well as attack instructions. Thus, the 2002/udp traffic can be used by a remote attacker as a communications channel between infected systems to co-ordinate attacks on other sites. ■

CERT Advisory CA-2002-27

kdelibs

A vulnerability was discovered in KDE's SSL implementation in that it does not check the basic constraints on a certificate and as a result may accept certificates as valid that were signed by an issuer who is not authorized to do so.

It can lead to Konqueror and other SSL-enabled KDE software falling victim to a man-in-the-middle attack without being aware of the invalid certificate. This will trick users into thinking they are on a secure connection with a valid site when in fact the site is different from that which they intended to connect to. The bug is fixed in KDE 3.0.3, and the KDE team provided a patch for KDE 2.2.2. ■

Mandrake reference MDKSA-2002:058

krb5

The network authentication system in Kerberos 5 contains an RPC library that includes an XDR decoder derived from Sun's RPC implementation. This implementation is vulnerable to a heap overflow. With Kerberos, it is believed that an attacker would need to be able to successfully authenticate to kadmin to be able to exploit this vulnerability. ■

Mandrake reference MDKSA-2002:057

Updated gaim client fixes URL vulnerability

Updated gaim packages are now available for Red Hat Linux 7.1, 7.2, and 7.3. These updates fix a vulnerability in the URL handler. Gaim is an all-in-one instant messaging client that lets you use a number of messaging protocols such as AIM, ICQ, and Yahoo, all at once.

Versions of gaim prior to 0.59.1 contain a bug in the URL handler of the manual browser option. A link can be carefully crafted to contain an arbitrary shell script which will be executed if the user clicks on the link. Users of gaim should update to the errata packages containing gaim 0.59.1 which is not vulnerable to this security issue. ■

Red Hat reference RHSA-2002:189-08

New wordtrans packages fix remote vulnerabilities

The wordtrans-web package provides an interface to query multilingual dictionaries via a web browser. Guardent Inc. has discovered vulnerabilities which affect versions up to and including 1.1pre8.

Improper input validation allows for the execution of arbitrary code or injection of cross-site scripting code by passing in unexpected parameters to the wordtrans.php script. The wordtrans.php script then unsafely executes the wordtrans binary with the malformed parameters. All users of wordtrans are advised to upgrade to the errata packages

Table 1: Security Posture of Major Distributions

Distributor	Security Sources	Comment
Debian	Info: *www.debian.org/security/*, List: debian-security-announce, Reference: DSA-... [1]	Debian have integrated current security advisories on their web site. The advisories take the form of HTML pages with links to patches. The security page also contains a note on the mailing list.
Mandrake	Info: *www.mandrakesecure.net*, List: security-announce, Reference: MDKSA-... [1]	MandrakeSoft run a web site dedicated to security topics. Amongst other things the site contains security advisories and references to mailing lists. The advisories are HTML pages, but there are no links to the patches.
Red Hat	Info: *www.redhat.com/errata/* List: *www.redhat.com/mailing-lists/* (linux-security and redhat-announce-list) Reference: RHSA-... [1]	Red Hat categorizes security advisories as Errata: Under the Errata headline any and all issues for individual Red Hat Linux versions are grouped and discussed. The security advisories take the form of HTML pages with links to patches.
SCO	Info: *www.sco.com/support/security/*, List: *www.sco.com/support/forums/announce.html*, Reference: CSSA-... [1]	You can access the SCO security page via the support area. The advisories are provided in clear text format.
Slackware	List: *www.slackware.com/lists/* (slackware-security), Reference: slackware-security ...[1]	Slackware do not have their own security page, but do offer an archive of the Security mailing List.
SuSE	Info: *www.suse.de/uk/private/support/security/*, Patches: *www.suse.de/uk/private/download/updates/*, List: suse-security-announce, Reference: suse-security-announce ... [1]	There is a link to the security page on the homepage. The security page contains information on the mailing list and advisories in text format. Security patches for individual SuSE Linux versions are marked red on the general update page and comprise a short description of the patched vulnerability.

[1] Security mails are available from all the above-mentioned distributions via the reference provided.

which contain a patch to correct this problematic vulnerability.

Red Hat reference RHSA-2002:188-08

Updated ethereal packages are available

Ethereal is a package designed for monitoring network traffic on your system. A buffer overflow in Ethereal 0.9.5 and earlier allows remote attackers to cause a denial of service or execute arbitrary code via the ISIS dissector. Users of Ethereal should update to the errata packages containing Ethereal version 0.9.6 .

Red Hat reference RHSA-2002:170-12

i4l

The i4l package contains several programs for ISDN maintenance and connectivity on Linux. The ipppd program which is part of the package contained various buffer overflows and format string bugs. Since ipppd is installed setuid to root and executable by users of group 'dialout' this may allow attackers with appropriate group membership to execute arbitrary commands as root.

The i4l package is installed by default and also vulnerable if you do not have a ISDN setup. The buffer overflows and format string bugs have been fixed. We strongly recommend an update of the i4l package. If you do not consider updating the package it is also possible to remove the setuid bit from /usr/sbin/ipppd as a temporary workaround.

The SuSE Security Team is aware of a published exploit for ipppd that gives a local attacker root privileges so you should either update the package or remove the setuid bit from ipppd.

SuSE reference SuSE-SA:2002:030

glibc

An integer overflow has been discovered in the xdr_array() function, contained in the Sun Microsystems RPC/XDR library, which is part of the glibc library package on all SuSE products. This overflow allows a remote attacker to overflow a buffer, leading to remote execution of arbitrary code supplied by the attacker.

There is no temporary workaround for this security problem other than disabling all RPC based server and client programs. The permanent solution is to update the glibc packages.

SuSE reference SuSE-SA:2002:031

cacti

A problem in cacti, a PHP based front-end to rrdtool for monitoring systems and services, has been discovered. This could lead into cacti executing arbitrary program code under the user id of the web server.

The problem has been fixed by removing any dollar signs and backticks from the title string in version 0.6.7-2.1 for the current stable distribution (woody) and in version 0.6.8a-2 for the unstable distribution (sid).

Debian reference DSA-164-1