Insecurity News

WebFS

Jens Steube reported two vulnerabilities in webfs, a lightweight HTTP server for static content.

CAN-2003-0832: When virtual hosting is enabled, a remote client could specify ".." as the hostname in a request, allowing retrieval of directory listings or files above the document root.

CAN-2003-0833: A long pathname could overflow a buffer allocated on the stack, allowing execution of arbitrary code. In order to exploit this vulnerability, it would be necessary to be able to create directories on the server in a location that could be accessed by the web server. In conjunction with CAN-2003-0832, this could be a world-writable directory such as

```
/var/tmp
```

■

Debian reference DSA-392-1 webfs – buffer overflows, file and directory exposure

Hztty

Jens Steube reported a pair of buffer overflow vulnerabilities in hztty, a program to translate Chinese character encodings in a terminal session. These vulnerabilities could be exploited by a local attacker to gain root privileges on a system where hztty is installed.

Also, hztty had been incorrectly installed setuid root, when it only requires the privileges of group utmp. ■

Debian reference DSA-385-1 hztty – buffer overflows

SSH-krb5

Several bugs have been found in OpenSSH's buffer handling. It is not known if these bugs are exploitable, but as a precaution an upgrade is advised. DSA-383-2: This advisory is an addition to the earlier DSA-383-1 advisory: Solar Designer found four more bugs in OpenSSH that may be exploitable. ■

Debian reference DSA-383-2 ssh-krb5 – possible remote vulnerability

Security Posture of Major Distributions

Distributor	Security Sources	Comments
Debian	Info: *http://www.debian.org/security/* List: *http://lists.debian.org/debian-security-announce/* Reference: DSA-... 1)	The current Debian security advisories are included on the homepage. Advisories are provided as HTML pages with links to the patches. The security advisory also contains a reference to the mailing list.
Gentoo	Forum: *http://forums.gentoo.org/* List: *http://www.gentoo.org/main/en/lists.xml* Reference: GLSA: ... 1)	Unfortunately, Gentoo does not offer a website with security updates or other security information. This forum is the only alternative.
Mandrake	Info: *http://www.mandrakesecure.net* List: *http://www.mandrakesecure.net/en/mlist.php* Reference: MDKSA-... 1)	MandrakeSoft runs its own Web site on security topics. Among other things, it includes security advisories and references to the mailing lists. The advisories are HTML pages, but there are no links to the patches.
Red Hat	Info: *http://www.redhat.com/errata/* List: *http://www.redhat.com/mailing-lists/* Reference: RHSA-... 1)	Red Hat files security advisories as so-called Errata: Issues for each Red Hat Linux version are then grouped. The security advisories are provided in the form of an HTML page with links to patches.
Slackware	Info: *http://www.slackware.com/security/* List: *http://www.slackware.com/lists/* (slackware-security) Reference: [slackware-security] ... 1)	The start page contains links to the security mailing list archive. No additional information on Slackware security is available.
SuSE	Info: *http://www.suse.de/uk/private/support/security/* Patches: *http://www.suse.de/uk/private/download/updates/* List: suse-security-announce Reference: SUSE-SA ... 1)	There is no longer a link to the security page after changes to the Web site. It contains information on the mailing list and the advisories. The security patches for the individual SuSE Linux versions are shown in red on the general updates site. A short description of the vulnerability the patch resolves is provided

1) All distributors indicate security mails in the subject line.

Sendmail

Two vulnerabilities were reported in sendmail.

CAN-2003-0681: A "potential buffer overflow in ruleset parsing" for Sendmail 8.12.9, when using the non-standard rulesets (1) recipient (2), final, or (3) mailer-specific envelope recipients, has unknown consequences.

CAN-2003-0694: The prescan function in Sendmail 8.12.9 allows remote attackers to execute arbitrary code via buffer overflow attacks, as demonstrated using the parseaddr function in parseaddr.c. ■

Debian reference DSA-384-1 sendmail – buffer overflows
SuSE reference SuSE-SA:2003:040
Mandrake reference MDKSA-2003:092
Red Hat reference RHSA-2003:283

OpenSSL095

Steve Henson of the OpenSSL core team identified and prepared fixes for a number of vulnerabilities in the OpenSSL ASN1 code that were discovered after running a test suite by British National Infrastructure Security Co-ordination Centre (NISCC).

A bug in OpenSSLs SSL/TLS protocol was also identified. This causes OpenSSL to parse a client certificate from an SSL/TLS client, when it should reject it as a protocol error. The Common Vulnerabilities and Exposures project identifies the following problems:

CAN-2003-0543: Integer overflow in OpenSSL that allows remote attackers to cause a denial of service (crash) via an SSL client certificate with certain ASN.1 tag values.

CAN-2003-0544: OpenSSL does not properly track the number of characters in certain ASN.1 inputs, which allows remote attackers to cause a denial of service (crash) via an SSL client certificate that causes OpenSSL to read past the end of a buffer when the long form is used.

CAN-2003-0545: Double-free vulnerability allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an SSL client certificate with a certain invalid ASN.1 encoding. This bug was only present in OpenSSL 0.9.7 and is listed here only for reference. ■

Debian reference DSA-394-1 openssl095 – ASN.1 parsing vulnerability

XFree86

Four vulnerabilities have been discovered in Xfree86.

CAN-2003-0063: xterm window title reporting escape sequence can deceive user

CAN-2003-0071: xterm susceptible to DEC UDK escape sequence denial-of-service attack

CAN-2002-0164: flaw in X server's MIT-SHM extension permits user owning X session to read and write arbitrary shared memory segments

CAN-2003-0730: multiple integer overflows in the font libraries for XFree86 allow local or remote attackers to cause a denial of service or execute arbitrary code via heap-based and stack-based buffer overflow attacks ■

Debian reference DSA-380-1 xfree86 – buffer overflows, denial of service

Mandrake reference MDKSA-2003:089

KDEbase

Two vulnerabilities were discovered in kdebase:

CAN-2003-0690: KDM in KDE 3.1.3 and earlier does not verify whether the pam_setcred function call succeeds, which may allow attackers to gain root privileges by triggering error conditions within PAM modules, as demonstrated in certain configurations of the MIT pam_krb5 module.

CAN-2003-0692: KDM in KDE 3.1.3 and earlier uses a weak session cookie generation algorithm that does not provide 128 bits of entropy, which allows attackers to guess session cookies via brute force methods and gain access to the user session. ■

Debian reference DSA-388-1 kdebase – several vulnerabilities

Mandrake reference MDKSA-2003:091

Red Hat reference RHSA-2003:269

libmailtools-perl

During an audit, the SuSE security team discovered a bug in Mail::Mailer, a Perl module used for sending email, whereby potentially untrusted input is passed to a program such as mailx, which may interpret certain escape sequences as commands to be executed. ■

Debian reference DSA-386-1 libmailtools-perl – input validation bug

Red Hat reference RHSA-2003:256

Freesweep

Steve Kemp discovered a buffer overflow in freesweep, when processing several environment variables. This vulnerability could be exploited by a local user to gain gid 'games'. ■

Debian reference DSA-391-1 freesweep – buffer overflow

MySQL

MySQL, a popular relational database system, contains a buffer overflow condition which could be exploited by a user who has permission to execute "ALTER TABLE" commands on the tables in the "mysql" database. If successfully exploited, this vulnerability could allow the attacker to execute arbitrary code with the privileges of the mysqld process (by default, user "mysql"). Since the "mysql" database is used for MySQL's internal record keeping, by default the mysql administrator "root" is the only user with permission to alter its tables. ■

Debian reference DSA-381-1 mysql – buffer overflow

SuSE reference SuSE-SA:2003:042

Mandrake reference MDKSA-2003:094

Red Hat reference RHSA-2003:281

ipmasq

ipmasq is a package which simplifies configuration of Linux IP masquerading, a form of network address translation which allows a number of hosts to share a single public IP address. Due to use of certain improper filtering rules, traffic arriving on the external interface addressed for an internal host would be forwarded, regardless of whether it was associated with an established connection. This vulnerability could be exploited by an attacker capable of forwarding IP traffic with an arbitrary destination address to the external interface of a system with ipmasq installed. ■

Debian reference DSA-389-1 ipmasq – insecure packet filtering rules

Marbles

Steve Kemp discovered a buffer overflow in marbles, when processing the HOME environment variable. This vulnerability could be exploited by a local user to gain gid 'games'. ■

Debian reference DSA-390-1 marbles – buffer overflow

OpenSSL

Dr. Stephen Henson, using a test suite provided by NISCC, discovered a number of vulnerabilities in the OpenSSL ASN1 code.

Combined with an error that causes the OpenSSL code to parse client certificates even when it should not, these errors can cause a denial of service (DoS) condition on a system using the OpenSSL code, depending on how that code is used.

For example, even though apache-ssl and ssh link to OpenSSL libraries, they should not be affected by this vulnerability. ■

Debian reference DSA-393-1 openssl – denial of service

SuSE reference SuSE-SA:2003:043

Mandrake reference MDKSA-2003:098

Red Hat reference RHSA-2003:292

SSH

A bug has been found in OpenSSH's buffer handling, whereby a buffer could be marked as grown when the actual reallocation failed.

DSA-382-2: This advisory supplements to the earlier DSA-382-1 advisory: two more buffer handling problems have been found in addition to the one described in DSA-382-1. It is not known if these bugs are exploitable, but as a precaution, an upgrade is advised for all users.

DSA-382-3: This advisory supplements to the earlier DSA-382-1 and DSA-382-2 advisories: Solar Designer has found a further four more vulnerabilities in OpenSSH that may be exploitable. ■

Debian reference DSA-382-3 ssh – possible remote vulnerability

SuSE reference SuSE-SA:2003:039

Mandrake reference MDKSA-2003:098

Red Hat reference RHSA-2003:279

Gopher

gopherd, a gopher server from the University of Minnesota, contains a number of buffer overflow vulnerabilities which could be exploited by a remote attacker. These could be used to execute arbitrary code on the target system with the privileges of the gopherd process (the "gopher" user by default). ■

Debian reference DSA-387-1 gopher – buffer overflows