# InSecurity News

## Kerberos

Durch mehrere Buffer Overflows in MIT Kerberos 5 kann ein entfernter Angreifer Root-Rechte erlangen. Der Fehler in der »krb5_aname_to_localname()«-Funktion lässt sich aber nur schwer ausnutzen, auch ist die Standardkonfiguration nicht anfällig. Nur Systeme mit explizitem Mapping und regelbasiertem Mapping sind betroffen.

Fehlerhaft ist MIT Kerberos in den Versionen 5-1.3.3 und älter. Alle im Paket befindlichen Programme (etwa »ftp«, »rsh«, »rlogin«, »telnet« und »ksu«) enthalten diese Schwachstellen. [http://www.securityfocus.com/bid/10448] ■

## Tripwire

Wegen eines Format-String-Fehlers in Tripwire kann ein lokaler Angreifer unter Umständen Root-Rechte erlangen. Der Programmierfehler in »pipedmailmessage.cpp« tritt auf, wenn Tripwire eine E-Mail generiert.

Ein Angreifer kann dies ausnutzen, indem er eine Datei mit manipuliertem Namen auf dem System erzeugt. Die Reportfunktion von Tripwire bindet diesen Name in die Mail ein, die sie dem Admin schickt. Dabei kommt es zu dem Format-String-Problem. Betroffen sind die Versionen 4.2 und älter. [http://www.securityfocus.com/bid/10454] ■

## Opera und Konqueror

Durch eine Schwachstelle beim Verarbeiten von Telnet-URLs in Opera kann ein entfernter Angreifer Befehle auf dem Client-System ausführen. Er erhält die Rechte des Opera-Anwenders. Das Problem tritt auf, wenn eine Webseite URLs wie »telnet://-n*Dateiname*« verwendet.

Die eingeschmuggelte Option »-n« sorgt dafür, dass das Telnet-Programm eine Loggingdatei im Homeverzeichnis des Opera-Anwenders anlegt. Betroffen davon sind die Versionen vor 7.50 (getestet auf 7.23). [http://www.idefense.com/application/poi/display?id=104&type=vulnerabilities]

Für das gleiche Problem ist auch Konqueror in KDE 3.2.2 und älter anfällig. [http://www.securitytracker.com/alerts/2004/May/1010173.html]

Ein weiteres Problem in Opera führt dazu, dass ein entfernter Angreifer den Browser dazu bringen kann, eine beliebige URL in der Statuszeile anzuzeigen. Ein Angreifer muss hierzu einen URL-Redirect verwenden und diesen mit einem »BODY onUnload()«-Tag wieder abbrechen. Betroffen sind ebenfalls die Versionen vor 7.50 (getestet 7.23). [http://www.securitytracker.com/alerts/2004/May/1010154.html] ■

**Tabelle 1: Sicherheit bei den großen Distributionen**

| Distributor | Quellen zur Sicherheit | Bemerkungen |
|---|---|---|
| Debian | Infos: [http://www.debian.org/security/]<br>Liste: [http://lists.debian.org/debian-security-announce/]<br>Betreff: DSA-... [1] | Bei Debian sind die aktuellen Security Advisories bereits auf der Homepage zu finden. Die Meldungen sind als HTML-Seiten mit Links zu den Patches realisiert. Die Sicherheitsseite enthält auch Hinweise zur Mailingliste. |
| Gentoo | Infos: [http://www.gentoo.org/security/]<br>Liste: [http://www.gentoo.org/main/en/lists.xml] (gentoo-announce und gentoo-security)<br>Betreff: GLSA: ... [1] | Auf der Gentoo-Website ist seit dem Frühjahr 2004 ein eigener Bereich zu Sicherheitsaktualisierungen und anderen Security-Informationen zu finden. Die Sicherheitsseite ist vorbildlich auf der Homepage verlinkt. Die Advisories liegen als HTML-Seiten vor. |
| Mandrake | Infos: [http://www.mandrakesecure.net]<br>Liste: [http://www.mandrakesecure.net/en/mlist.php] (announce)<br>Betreff: MDKSA-... [1] | Mandrakesoft betreibt eine eigene Website zu Sicherheitsthemen. Sie enthält unter anderem Security Advisories und Hinweise zu den Mailinglisten. Die Advisories sind zwar HTML-Seiten, die Patches darin aber nicht verlinkt. |
| Red Hat | Infos: [http://www.redhat.com/security/]<br>Liste: [http://www.redhat.com/mailman/listinfo/] (Enterprise-watch-list und Redhat-watch-list)<br>Betreff: [RHSA-... [1] | Red Hat listet Security Advisories unter »Support I Security and Updates« für jede unterstützte Version, derzeit vor allem für die Enterprise-Ausgaben. Die Security Advisories liegen als HTML-Seite vor, die Patches sind darin aber nicht verlinkt. |
| Slackware | Infos: [http://www.slackware.com/security/]<br>Liste: [http://www.slackware.com/lists/] (slackware-security)<br>Betreff: [slackware-security] ... [1] | Die Startseite verlinkt direkt zum Archiv der Security-Mailingliste. Darüber hinaus sind auf der Homepage jedoch keine Informationen zur Sicherheit von Slackware zu finden. |
| Suse | Infos: [http://www.suse.de/security/]<br>Patches: [http://www.suse.de/de/support/download/updates/]<br>Liste: suse-security-announce<br>Betreff: [suse-security-announce] ... [1] | Die Sicherheitsseite ist nach einer Änderung der Homepage nicht mehr direkt verlinkt. Sie enthält Infos zur Mailingliste sowie die Advisories. Die Sicherheitspatches zu den einzelnen Suse-Linux-Versionen sind in der allgemeinen Updates-Seite rot markiert und mit einer kurzen Beschreibung der geschlossenen Lücke versehen. |
| | [1] Alle Distributoren kennzeichnen ihre Security-Mails im Betreff. | |

## PHP

Durch einen Fehler beim Verarbeiten von URLs kann ein entfernter Angreifer Filter-Restriktionen umgehen. Betroffen ist PHP bis 3.0.13. [http://www.securitytracker.com/alerts/2004/May/1010326.html]
Die PHP-Version in Slackware ist mit einer statischen Bibliothek in einem unsicheren Pfad verlinkt (hier »/tmp«). PHP sucht seine Shared Libraries dann auch in diesem Verzeichnis. Ein lokaler Angreifer kann eine Bibliothek an diesen Ort setzen und damit seinen Code einschleusen. Betroffen hiervon sind die Slackware-Versionen von PHP vor 4.3.6. [http://www.securitytracker.com/alerts/2004/Jun/1010368.html] ■

## BEA Weblogic Server und Express

Beim Bearbeiten von »weblogic.xml« entfernen Weblogic-Builder und die Funktion »SecurityRoleAssignmentMBean.toXML()« eventuell vorhandene »<security-role-assignment>«-Tags. Entfernte Angreifer können so unberechtigt Zugriff erhalten.
Betroffen sind die Versionen 8.1 SP2 (und älter) sowie 7.0 SP5 (und älter). [http://www.securitytracker.com/alerts/2004/May/1010128.html]
Ein weiterer Bug führt dazu, dass ein entfernter, angemeldeter Angreifer mit Admin- oder Operator-Rechten unberechtigt Server starten oder stoppen kann. Voraussetzung: Der Admin hat die Sicherheitseinstellungen für das Starten und Stoppen von Servern geändert. Betroffen sind ebenfalls die Versionen bis 8.1 SP2 und bis 7.0 SP5. [http://www.securitytracker.com/alerts/2004/May/1010129.html] ■

## Ethereal

Im Netzwerksniffer Ethereal wurden mehrere Schwachstellen entdeckt. Sie finden sich in Codeteilen, die für das Handling der folgenden Protokolle zuständig sind: SIP, AIM, SPNEGO und MMSE. Ein entfernter Angreifer kann diese Lücken ausnutzen, um Befehle mit den Rechten des Ethereal-Prozesses auszuführen. Betroffen sind Versionen 0.9.8 bis 0.10.3 einschließlich. [http://www.securityfocus.com/bid/10347] ■

## Neon

In der HTTP- und Webdav-Bibliothek Neon wurde ein Sicherheitsproblem gefunden. Ein entfernter Angreifer kann Befehle auf dem System ausführen, weil in den Parsing-Routinen ein Heap-Overflow auftritt (in der »ne_rfc1036_parse()«-Funktion). Die Befehle laufen mit den Rechten der jeweiligen Anwendung. Betroffen sind die Versionen 0.24.5 und älter. [http://security.e-matters.de/advisories/062004.html] ■

## Firebird und Interbase

Ein entfernter Angreifer kann Firebird zum Absturz bringen. Dazu muss er eine Verbindung zur Datenbank öffnen und einen speziellen Datenbanknamen senden: »gsec -database *Datenbank-IP*:`perl -e'print ("A"x300)'` -user *Blabla* -password *Blupp*«. Als Datenbankname sendet dieses Kommando einen String, der aus 300 »A«-Zeichen besteht. Betroffen ist die Firebird-Version 1.0. [http://www.securityfocus.com/bid/10446]
Ein ähnlicher Fehler findet sich in Borlands Interbase-Datenbank 7.1.0. [http://www.securitytracker.com/alerts/2004/Jun/1010381.html] ■

## PHP-Nuke

Im Contentmanagement-System PHP-Nuke wurden mehrere Sicherheitslecks entdeckt. Durch Fehler beim Verarbeiten einiger Variablen kann ein entfernter Angreifer Cross-Site-Skripting-Attacken ausführen. Betroffen hiervon sind die »optionbox«-Variable im News-Modul, die »date«-Variable im Statistics-Modul und einige weitere Variablen in den Stories_Archive- und Surveys-Modulen.
Auch das Union-Tap-Prevention-Feature ist anfällig. Betroffen hiervon sind die Versionen 6.x bis 7.3. [http://www.securitytracker.com/alerts/2004/May/1010177.html]
Ein Include-Bug führt dazu, dass ein entfernter Angreifer Befehle mit Webserver-Rechten ausführen kann. PHP-Nuke initialisiert die Variable »modpath« nicht richtig, so kann ein Angreifer eigene Include-Dateien einschleusen. [http://www.securitytracker.com/alerts/2004/May/1010186.html]
Durch eine Schwachstelle im »mainfile.php«-Skript kann ein lokaler Angreifer SQL-Injection-Attacken ausführen. Ein Exploit findet sich unter der angegebenen Adresse. [http://www.securitytracker.com/alerts/2004/Jun/1010351.html]
Mit »http://*Zielhost*/admin/case/case.adminfaq.php/admin.php?op=FaqCatGo« erfährt ein entfernter Angreifer den Installationspfad. Betroffen von dieser Schwachstelle sind rund 140 Skripte in Version 7.3 und älter. [http://www.securitytracker.com/alerts/2004/Jun/1010355.html]
Weitere Eingabekontrollfehler im Reviews-Modul beim Verarbeiten der »id«- und »title«-Variablen führen dazu, dass einem entfernten Angreifer Cross-Site-Skripting-Attacken gelingen. Betroffen sind die Versionen 6.x, 7.2 und 7.3. [http://www.securitytracker.com/alerts/2004/Jun/1010420.html]
Zahlreiche weitere Schwachstellen erlauben Cross-Site-Skripting-Angriffe in den Versionen 6.x bis 7.3. [http://www.securitytracker.com/alerts/2004/Jun/1010477.html] ■

## Cpanel

Ein lokaler Angreifer kann Befehle mit den Rechten anderer Benutzer ausführen, falls Cpanel mit der Apache-Option »mod_phpsuexec« verwendet wird. Der Exploit nutzt dafür die Variable »PATH_INFO«. [http://www.securitytracker.com/alerts/2004/May/1010270.html]

Ein entfernter, angemeldeter Administrator kann DNS-Informationen anderer Accounts löschen. Er nutzt »/scripts/killacct« mit einem Cookie. [http://www.securitytracker.com/alerts/2004/Jun/1010398.html]

Ein entfernter, angemeldeter Angreifer kann aufgrund eines Fehlers in SU-Exec Befehle mit den Rechten anderer Benutzer ausführen. Betroffen sind die Versionen 9.3.0-EDGE_95 und älter. [http://www.securitytracker.com/alerts/2004/Jun/1010411.html]

Außerdem kann ein entfernter Angreifer das Datenbank-Passwort nach Belieben setzen, er nutzt dazu »http://*Zielhost*:2086/scripts/passwd« mit einigen Parametern. [http://www.securitytracker.com/alerts/2004/Jun/1010449.html] ■

## Webmin

In Webmin wurden zwei Sicherheitslücken entdeckt. Ein entfernter Angreifer kann fremde Benutzer aussperren, indem er ungültige Accountdaten an den Webmin-Server sendet.

Die zweite Schwachstelle erlaubt es angemeldeten, entfernten Angreifern, sich die Konfigurationsdaten von Modulen anzusehen. Betroffen sind die Webmin-Versionen 1.140 und älter. [http://www.securitytracker.com/alerts/2004/Jun/1010422.html] ■

## Apache-Module

Per Buffer Overflow im Apache-Modul Mod_ssl kann ein entfernter Angreifer Befehle mit Webserver-Rechten ausführen. Der Overflow in »ssl_util_uuencode_binary()« lässt sich per Subject DN nutzen. [http://www.securitytracker.com/alerts/2004/May/1010322.html]

Auch in Mod_proxy findet sich ein Buffer Overflow, er tritt beim Verarbeiten des HTTP-Content-Length-Feldes auf. Betroffen ist Apache 1.3.31. [http://www.guninski.com/modproxy1.html] ■

**Tabelle 2: Linux-Advisories vom 14.05. bis 19.06.04** — **In Zusammenarbeit mit dem DFN-CERT**

Zusammenfassungen, Diskussionen und die vollständigen Advisories sind unter [http://www.linux-community.de/story?storyid=*ID*] zu finden.

| ID | Linux | Beschreibung | ID | Linux | Beschreibung |
|---|---|---|---|---|---|
| 13337 | Suse | »mc«-Dateimanager | 13508 | Generisch | »FakeBasicAuth«-Funktionen von Mod_ssl |
| 13338 | Debian | Mah-jong-Spiel | 13510 | Debian | Fftpgw |
| 13375 | Red Hat | Kdelibs | 13515 | Debian | Gatos / Xatitv |
| 13377 | Mandrake | Libuser | 13516 | Debian | Ethereal |
| 13378 | Mandrake | Passwd | 13527 | Mandrake | Xpcd-Svga |
| 13379 | Debian | Kerberos-4-Komponente von Heimdahl | 13528 | Mandrake | Mod_ssl / Apache 1.3 |
| 13389 | Debian | Neon-Bibliothek | 13529 | Mandrake | Mod_ssl / Apache 2 |
| 13390 | Red Hat | Cadaver-Pakete | 13534 | Generisch | Mapping-Funktionalität von MIT Kerberos 5 |
| 13393 | Debian | CVS-Server | 13535 | Debian | Rsync |
| 13394 | Red Hat | CVS-Server | 13536 | Debian | Gallery |
| 13395 | Suse | CVS-Server | 13547 | Mandrake | Mapping-Funktionalität von MIT Kerberos 5 |
| 13397 | Mandrake | Apache 1.3 | 13549 | Debian | Log2mail |
| 13409 | Mandrake | CVS-Server | 13550 | Red Hat | CVS-Server |
| 13410 | Mandrake | Kdelibs | 13577 | Debian | Debian-2.2-Kernel |
| 13411 | Mandrake | Neon-Bibliothek | 13578 | Debian | LHA-Programm |
| 13412 | Debian | Cadaver-Pakete | 13579 | Debian | ODBC-Treiber von PostgreSQL |
| 13413 | Mandrake | Update: Apache 1.3 | 13588 | Red Hat | Squid |
| 13414 | Red Hat | »mc« (Midnight Commander) | 13589 | Red Hat | Ethereal-Paket-Dissektoren |
| 13415 | Red Hat | Libpng | 13590 | Red Hat | CVS-Server |
| 13416 | Red Hat | Rsync | 13591 | Suse | CVS-Server |
| 13419 | Red Hat | MC-Pakete | 13605 | Suse | Squid-NTLM-Authentifizierung |
| 13420 | Red Hat | Mutt | 13606 | Red Hat | Mapping-Funktionalität von MIT Kerberos 5 |
| 13421 | Red Hat | Pwlib | 13607 | Mandrake | Update: Mapping-Funktionalität von MIT Kerberos 5 |
| 13422 | Red Hat | Metamail | 13608 | Mandrake | CVS-Server |
| 13423 | Red Hat | Utempter | 13609 | Mandrake | Squid-NTLM-Authentifizierung |
| 13424 | Red Hat | Libtool | 13615 | Generisch | Oracle E-Business-Suite |
| 13441 | Debian | Xpcd-Svga | 13619 | Mandrake | Ksymoops-»gznm«-Skript |
| 13443 | Mandrake | Kernel 2.6 | 13639 | Debian | CVS-Server |
| 13445 | SGI | Linux-Kernel des Altix Propack 3 | 13640 | Debian | KDE (Kdelibs) |
| 13446 | SGI | Linux-Kernel des Altix Propack v2.4 | 13644 | Red Hat | Apache-Httpd- und Mod_ssl-Pakete |
| 13468 | Red Hat | Tcpdump-Pakete | 13645 | Red Hat | Squirrelmail |
| 13469 | Red Hat | Utempter-Pakete | 13646 | Red Hat | Tripwire |
| 13470 | Red Hat | LHA-Pakete | 13647 | Debian | CVS-Server |
| 13477 | Mandrake | Kolab (KDE-Groupware-Server) | 13668 | Debian | Mapping-Funktionalität von MIT Kerberos 5 |
| 13478 | Mandrake | Mailman | 13670 | Suse | Subversion |
| 13479 | Generisch | HP Openview Select Access | 13672 | Suse | Linux-Kernel 2.4 und 2.6 |
| 13485 | SGI | Propack 3 | 13679 | Red Hat | Linux-Kernel |

## Kurzmeldungen

**Libtasn1** 0.1.x (vor 0.1.2), 0.2.x (vor 0.2.7): Parsing-Fehler beim Verarbeiten von ASN.1-DER-Daten, Auswirkungen abhängig von der jeweiligen Applikation. [http://www.securityfocus.com/bid/10360]

**Zen Cart** 1.1.2d: Fehler beim Filtern der Eingabe in »admin/login.php«, SQL-Injection möglich. [http://www.securityfocus.com/bid/10378]

**Turbo Traffic Trader C** 1.0: Fehler beim Verarbeiten von URLs, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/10359]

**Sun Java Secure Socket Extension** 1.0.3, 1.0.3_01 und 1.0.3_02: Fehler im Authentifizierungsprozess, validiert Server trotz ungültigen Zertifikats. [http://www.securitytracker.com/alerts/2004/May/1010193.html]

**Zone-Minder** vor 1.19.2: Buffer Overflow im »zms«-Programm, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/10340]

**Phorum** 4.3.7: Anmeldeprozess anfällig für Replay-Attacken, entfernter Angreifer kann Sitzung anderer User übernehmen (Session Hijacking). [http://www.securitytracker.com/alerts/2004/May/1010219.html]

**Liferay Enterprise Portal:** Eingabekontrollfehler in nahezu allen Eingabefeldern, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/10402]

**Busybox:** Fehler beim Arbeiten mit Netlink-Sockets, lokaler Angreifer kann Netlink-Nachrichten fälschen. [http://www.securitytracker.com/alerts/2004/May/1010272.html]

**XFree86 XDM:** Fehler in »xc/programs/xdm/socket.c« beim Handling von TCP-Sockets, öffnet TCP-Ports trotz deaktiviertem »DisplayManager.requestPort«. [http://www.securityfocus.com/bid/10423]

**Land Down Under** 700: Fehler beim Verarbeiten von BB-Codes, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/May/1010335.html]

**Jftpgw** vor 0.13.4: Format-String-Fehler in »log()«-Funktion, entfernter Angreifer kann Befehle mit den Rechten des Proxy-Daemon ausführen. [http://www.securitytracker.com/alerts/2004/May/1010338.html]

**Squirrel-Mail** vor 1.4.3 und vor 1.5.1 : Fehler beim Verarbeiten bestimmter Mails, Cross-Site-Skripting möglich. [http://www.rs-labs.com/adv/RS-Labs-Advisory-2004-1.txt]

**Gallery** 1.2 bis 1.4.3-pl1: Authentifizierungsfehler, entfernter Angreifer erlangt Admin-Rechte. [http://www.securityfocus.com/bid/10451]

**Mail Manage EX** 3.1.8: Fehler beim Verarbeiten der »Settings«-Variable, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securitytracker.com/alerts/2004/Jun/1010384.html]

**Un-RAR** vor 3.0: Format-String-Fehler in »getopt.c«-Datei, entfernter Angreifer kann Befehle mit den Rechten des Un-RAR-Anwenders ausführen. [http://www.securityfocus.com/bid/10442]

**Oracle E-Business-Suite** 11.0.x, 11.5.1 bis 11.5.8: Mehrere Eingabekontrollfehler, SQL-Injection möglich. [http://www.securitytracker.com/alerts/2004/Jun/1010400.html]

**Gnocatan** 0.6.1: Mehrere Buffer Overflows, entfernter Angreifer kann Befehle mit den Rechten des Gnocatan-Servers ausführen. [http://www.securitytracker.com/alerts/2004/Jun/1010416.html]

**JCIFS** vor 0.9.1: Authentifizierungsfehler falls ein Guest-Account vorhanden, ein entfernter Angreifer erlangt unberechtigt Zugriff. [http://www.securityfocus.com/bid/10494]

**Invision Power Board** 1.3.1 Final: Eingabekontrollfehler im »ssi.php«-Skript, SQL-Injection möglich. [http://www.securitytracker.com/alerts/2004/Jun/1010448.html]

**Surge-Mail** 1.9 (und älter): Verschiedene Eingabekontrollfehler, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/10483]

**J-Portal:** Eingabekontrollfehler in »module/print.inc.php«, SQL-Injection möglich. [http://www.securityfocus.com/bid/10430]

## L2tpd

Im L2TP-Daemon tritt ein Buffer Overflow in der Funktion »write_packet()« auf (in »control.c«). Um ihn auszunutzen, muss ein entfernter Angreifer einen L2TP-Tunnel aufbauen und durch ihn spezielle Daten senden. Die Schwachstelle ist jedoch nur schwierig auszunutzen; es ist sogar unklar, ob ein Angriff überhaupt möglich ist, und wenn ja, welche Folgen er hätte. Betroffen ist die L2tpd-Version 0.64. [http://www.securityfocus.com/bid/10466] ■

## CVS und Subversion

In CVS wurden mehrere Fehler gefunden. Beim Verarbeiten von Eingabezeilen tritt ein Heap Overflow auf, wenn CVS den Eingabestring um Modified- oder Unchanged-Flags ergänzt. Ein entfernter Angreifer kann Befehle mit den Rechten des CVS-Servers ausführen. Betroffen sind CVS 1.11.15 stable (und älter) sowie 1.12.7 feature (und älter). [http://security.e-matters.de/advisories/072004.html]

Da sich durch ein älteres Patch ein neuer Fehler in CVS eingeschlichen hatte, untersuchten zwei Sicherheitsexperten den CVS-Code genauer und fanden noch fatalere Lücken. Einen Fehler beim Allozieren von Speicher in der »error_prog _name()«-Funktion kann ein entfernter Angreifer per »Argumentx«-Befehl nutzen, um Befehle in den Server einzuschleusen. Eine weitere Lücke findet sich in »serve_notify()«. Die Funktion hat Probleme beim Verarbeiten von leeren Dateneinträgen. Ein entfernter Angreifer kann auch hier Befehle ausführen. Ein Integer Overflow im CVS-Protokollbefehl Max-Dotdot führt zum Absturz des Servers.

Ein Format-String-Fehler in »wrapper.c« führt dazu, dass ein entfernter Angreifer den CVS-Server abstürzen lassen kann. Weitere Fehlerangaben unter: [http://security.e-matters.de/advisories/092004.html]

Auch das CVS-ähnliche Programm Subversion enthält Sicherheitslücken. Ein entfernter Angreifer kann Befehle einschleusen. Der Overflow tritt auf, wenn der Angreifer eine spezielle »DAV2 REPORT«-Anfrage stellt. Betroffen sind die Versionen bis 1.0.2. [http://security.e-matters.de/advisories/082004.html]

Ein weiterer Heap Overflow tritt beim Verarbeiten des »svn://«-Protokolls auf. Ein entfernter Angreifer kann dadurch Befehle mit den Rechten des Subversion-Prozesses ausführen. Betroffen davon sind die Versionen 1.0.4 und älter. [http://subversion.tigris.org/security/CAN-2004-0413-advisory.txt] *(M. Vogelsberger/fjl)* ■

### Neue Releases

**Weplab:** WEP Testing Lab, eine Testsuite für die sehr unsichere WLAN-Verschlüsselungstechnik Wired Equivalent Privacy. [http://weplab.sf.net]

**Publimark:** Dieses Steganographie-Programm versteckt Daten in Audiofiles. [http://perso.wanadoo.fr/gleguelv/soft/]

### Kurzmeldungen

**HP Openview Select Access** 5.0 Patch 4, 5.1 Patch 1, 5.2 und 6.0: Fehler beim Verarbeiten von UTF-8-Zeichen in URLs, entfernter Angreifer kann auf gesperrte URLs zugreifen. [http://www.securitytracker.com/alerts/2004/May/1010275.html]

**Tivoli Access Manager** for E-Business 3.9, 4.1 und 5.1 sowie Identity Manager Solution 5.1: Fehler beim Verarbeiten von Cookies, entfernter Angreifer kann fremde Sitzungen übernehmen (Session Hijacking). [http://www.securitytracker.com/alerts/2004/May/1010379.html]

**Horde-IMP** vor 3.2.4: Fehler beim Verarbeiten von Maildaten, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/10501]

**Ksymoops** 2.4: Symlink-Fehler beim Anlegen temporärer Dateien in »/tmp«, lokaler Angreifer kann fremde Dateien überschreiben. [http://www.securityfocus.com/bid/10516]

**Wget** 1.9 und 1.9.1: Symlink-Schwachstelle, lokaler Angreifer kann Dateien mit den Rechten des Wget-Anwenders überschreiben oder neu erzeugen. [http://www.securityfocus.com/bid/10361]

**OS-Commerce:** Double-Dot-Fehler, entfernter Angreifer kann Files mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/10364]

**Xpcd:** Buffer Overflow, lokaler Angreifer kann Befehle mit den Rechten des Xpcd-Anwenders ausführen. [http://www.securitytracker.com/alerts/2004/May/1010260.html]

**Mailman** 2.1 vor 2.1.4: Als Antwort auf eine manipulierte Mail sendet Mailman das Passwort eines beliebigen Benutzers an den Angreifer. [http://www.securityfocus.com/bid/10412]

**Isoqlog:** Mehrere Buffer-Overflow-Schwachstellen, entfernter Angreifer kann durch überlange Maillog-Einträge Befehle mit den Rechten des Isoqlog-Anwenders ausführen. [http://www.securitytracker.com/alerts/2004/May/1010292.html]

**Spamguard** vor Version 1.7-Beta: Mehrere Buffer-Overflow-Fehler, entfernter Angreifer kann Befehle auf dem betroffenen System ausführen. [http://www.securityfocus.com/bid/10434]

**Log2mail** vor 0.2.5.2 (Debian-Versionsnummer): Format-String-Fehler, Angreifer kann Befehle mit »adm«-Gruppenrechten ausführen. [http://www.securityfocus.com/bid/10460]

**ODBC-Treiber in PostgreSQL** 07.03.0200-2 und älter: Buffer Overflow, entfernter Angreifer kann die ODBC-Applikation abstürzen lassen. [http://www.securityfocus.com/bid/10470]

**Roundup** vor 0.7.3: Double-Dot-Bug, entfernter Angreifer kann Files mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/10495]

**Squid** 3.x-PRE und 2.5.x: Buffer Overflow beim Verarbeiten von NTLM-Authentifizierungsnachrichten, entfernter Angreifer kann eigene Befehle einschleusen. [http://www.securityfocus.com/bid/10500]

**GNU Aspell** 0.50.5 und älter: Buffer Overflow im »word-list-compress«-Programm, Angreifer kann Befehle mit den Rechten des Aspell-Anwenders ausführen. [http://www.securityfocus.com/bid/10497]

**Smtp.proxy** 1.1.3 und älter: Format-String-Schwachstelle beim Verarbeiten einer manipulierten E-Mail, entfernter Angreifer kann Befehle mit den Rechten des »smtp.proxy«-Prozesses ausführen. [http://www.securityfocus.com/bid/10509]

**Gatos Xatitv 0.0.5:** Ruft »system()« mit Benutzerdaten auf, ohne vorher Root-Rechte abzugeben, lokaler Angreifer kann Befehle mit Root-Rechten ausführen. [http://www.securityfocus.com/bid/10437]

**Linux-Kernel** vor 2.4.26: Integer Overflow in »sctp_setsockopt()« bei gesetzter Socket-Option »SCTP_SOCKOPT_DEBUG_NAME«, lokaler Angreifer kann Befehle mit Kernel-Rechten ausführen. [http://www.securitytracker.com/alerts/2004/May/1010130.html]

**E-1000-Treiber** im Linux-Kernel vor 2.4.27-pre1: Buffer Overflow, lokaler Angreifer kann Befehle mit höheren Rechten ausführen. [http://www.securitytracker.com/alerts/2004/May/1010273.html]