InSecurity News

SSMTP

Zwei Format-String-Fehler in SSMTP führen dazu, dass ein entfernter Angreifer Befehle mit den Rechten des Daemon ausführen kann. Die schwachen Stellen treten in den Funktionen »die()« und »log_event()« auf. Betroffen sind die Versionen vor 2.50.6.1. [http://www.securitytracker.com/alerts/2004/Apr/1009788.html]

Durch einen Symlink-Bug beim Anlegen von »/tmp/ssmtp.log« kann ein lokaler Angreifer Dateien mit den Rechten des SSMTP-Prozesses überschreiben. Betroffen ist Version 2.50.6. [http://www.securitytracker.com/alerts/2004/Apr/1009883.html] ■

Xine und MPlayer

Im Xine-Player und in M-Player sind einige Buffer-Overflow-Schwachstellen zu finden. Sie treten beim Real-time Streaming Protocol auf (RTSP). Ein entfernter Angreifer mit Kontrolle über einen Streaming-Server kann Befehle auf den verbundenen Client-Systemen ausführen. Sie laufen mit den Rechten des Xine/MPlayer-Benutzers. Betroffen sind Xine-lib 1-beta1 bis 1-rc3c und MPlayer 1.0pre1-pre3try2. [http://www.securityfocus.com/bid/10245] ■

Exim

Im Exim-Mailserver wurden zwei Buffer-Overflow-Fehler entdeckt. Der Überlauf in »accept.c« lässt sich ausnutzen, falls »headers_check_syntax« in »exim.conf« aktiviert ist. Ein Fehler in »verify.c« tritt nur auf, wenn »require verify = header_syntax« gesetzt ist. Betroffen sind Exim 3.35 und 4.32. [http://www.guninski.com/exim1.html] ■

Squirrelmail

Ein Programmierfehler in dem Change_password-Plug-in der Webmail-Software Squirrelmail führt dazu, dass lokale Angreifer Befehle mit Root-Rechten ausführen können. Das Plugin-Hilfsprogramm »chpasswd« ist mit Set-UID-Root-Rechten installiert. In ihm tritt ein Buffer Overflow auf. [http://www.securitytracker.com/alerts/2004/Apr/1009860.html]

Durch einen Eingabekontrollfehler kann ein entfernter Angreifer auch Cross-Site-Skripting durchführen. Betroffen hiervon ist die Version 1.4.2. [http://www.securitytracker.com/alerts/2004/Apr/1010007.html]

Tabelle 1: Sicherheit bei den großen Distributionen

Distributor	Quellen zur Sicherheit	Bemerkungen
Debian	Infos: [http://www.debian.org/security/] Liste: [http://lists.debian.org/debian-security-announce/] 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/] Liste: [http://www.gentoo.org/main/en/lists.xml] (gentoo-announce und gentoo-security) 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] Liste: [http://www.mandrakesecure.net/en/mlist.php] (announce) 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/] Liste: [http://www.redhat.com/mailman/listinfo/] (Enterprise-watch-list und Redhat-watch-list) 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/] Liste: [http://www.slackware.com/lists/] (slackware-security) 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/] Patches: [http://www.suse.de/de/support/download/updates/] Liste: suse-security-announce 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.

Postnuke

In Postnuke wurden mehrere Sicherheitslücken gefunden. Das NS-Comments-Modul filtert die »sid«-Variable nicht korrekt, ein entfernter Angreifer kann daher SQL-Injection und Cross-Site-Skripting durchführen.
NS-Your_Account verarbeitet die »timezoneoffset«-Variable nicht korrekt. Ein entfernter, angemeldeter Angreifer kann daher SQL-Injection durchführen und Account-Informationen von Benutzern ändern. Ein Exploit wurde bereits veröffentlicht: [http://www.scan-associates.net/papers/post_nuker.php.txt]. Betroffen sind die Version 0.726 und ältere. [http://www.securitytracker.com/alerts/2004/Apr/1009801.html]
Das NS-Polls-Modul filtert die »pn_uid«-Variable nicht ordentlich. Wieder gelingt einem entfernten Angreifer SQL-Injection. Bugs beim Filtern der »order«-Variable führen dazu, dass ein entfernter Angreifer Cross-Site-Skripting durchführen kann. Eine zu aussagefreudige Fehlermeldung im Past_Nuke-Modul verrät den Installationspfad. Betroffen davon ist die Version 0.7.2.6. [http://www.securitytracker.com/alerts/2004/Apr/1009851.html]
Weitere Bugs in anderen Modulen, aber mit den gleichen Folgen, wurden in Postnuke 0.726 Phoenix gefunden. [http://www.securitytracker.com/alerts/2004/Apr/1009902.html] ■

Real-One und Realplayer

Durch einen Buffer Overflow in Realplayer und in Real-One kann ein entfernter Angreifer Befehle einschleusen. Diese laufen mit den Rechten des Real-Anwenders. Der Overflow tritt beim Verarbeiten von R3T-Dateien auf. Ein Angreifer sendet eine manipulierte R3T-Datei an sein Opfer, das nichts ahnend die gewünschten Befehle ausführt. [http://www.securityfocus.com/bid/10070] ■

CVS

Ein Fehler in CVS erlaubt es einem entfernten Angreifer, der Kontrolle über einen CVS-Server ausübt, Dateien auf den angebundenen Clients zu manipulieren.
Der Programmierfehler liegt in den CVS-Routinen, die Pfadnamen in RCS-Diff-Dateien verarbeiten. Der Server kann daher beim CVS-Checkout oder -Update absolute Pfade angeben. Betroffen ist Version 1.11.15. [http://www.securitytracker.com/alerts/2004/Apr/1009781.html]
Durch einen weiteren Fehler kann ein entfernter, angemeldeter Angreifer beliebige RCS-Dateien des Servers lesen. Betroffen ist die CVS-Version 1.11.15. [http://www.securitytracker.com/alerts/2004/Apr/1009853.html] ■

Pax

Die Sicherheitspatches Pax enthalten eine Lücke, durch die ein lokaler Angreifer einen Denial of Service durchführen kann. Die Schwachstelle tritt nur bei aktiviertem ASLR (Address Space Layout Randomization) auf. Betroffen sind Pax-Versionen vor 2.6. [http://www.securityfocus.com/bid/10264] ■

LCD-Proc

Durch einen Buffer Overflow in der »parse_all_client_messages()«-Funktion von LCD-Proc (Version 0.4.4) kann ein entfernter Angreifer Befehle mit den Rechten des LCD-Proc-Prozesses ausführen. [http://www.securitytracker.com/alerts/2004/Apr/1009712.html]
Ein weiterer Buffer Overflow sowie ein Format-String-Fehler finden sich in der Funktion »test_func_func()«. Ein Angreifer kann damit ebenfalls Befehle mit den Rechten des LCD-Proc-Prozesses ausführen. Betroffen sind die Version 0.4.1 und ältere. [http://www.securitytracker.com/alerts/2004/Apr/1009713.html] ■

Neue Releases

SQL Injection Signatures Evasion: Das Paper beschreibt, wie SQL-Injection-Attacken gegen vermeintlich davor geschützte Anwendungen dennoch möglich sind. [http://www.imperva.com/adc/papers/sigevasion/]

Anti-Exploit: Perl-Programm, das (ähnlich einem Virenscanner) nach bekannten Exploits auf dem lokalen System sucht. Es erkennt derzeit über 1400 verdächtige Dateien. [http://www.h07.org/projects/aexpl/]

Tabelle 2: Linux-Advisories vom 16.04. bis 13.05.04

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

ID	Linux	Beschreibung
12978	Red Hat	Schwachstelle in Squid
12979	Red Hat	Schwachstelle in Mailman
12980	Debian	Schwachstellen in MySQL
12982	Debian	Schwachstelle in SSMTP
12983	Red Hat	Schwachstelle in Subversion
12986	Debian	Schwachstelle im Spiel Xonix
13007	Debian	Schwachstellen in Suidperl
13009	Debian	Schwachstellen in CVS
13010	Debian	Schwachstelle in Neon-Bibliothek
13011	Debian	Race Condition in Logcheck
13012	Debian	Schwachstellen im Linux-2.4-Kernel für Mips
13013	Debian	Schwachstelle in Zope
13014	Debian	Schwachstellen im 2.4.19er Linux-Kernel für Mips
13015	Debian	Denial-of-Service-Schwachstelle in IProute
13023	Mandrake	Schwachstelle in Utempter
13024	Mandrake	Schwachstelle in Neon-Bibliothek
13025	Mandrake	Race Condition in Xine-UI
13026	Mandrake	Schwachstellen in MySQL
13027	Mandrake	Schwachstelle in Samba
13056	Generisch	Annahme gefälschter TCP-Segmente
13065	SGI	Linux-Sicherheitsupdate #18
13071	Debian	Buffer Overflow in XChat
13072	Debian	Buffer Overflow in Ident2
13076	Red Hat	Schwachstellen im IA64-Kernel in Red Hat Linux
13078	Red Hat	Schwachstellen in XFree86
13079	Red Hat	Schwachstellen im Linux-Kernel
13080	Red Hat	Schwachstellen im Kernel
13082	Mandrake	Update: Schwachstelle in Utempter/XChat
13083	Mandrake	Buffer Overflow in XChat
13087	Red Hat	Zwei Schwachstellen im Linux-Kernel
13120	Debian	Update zur Schwachstelle im 2.4.16er Linux-Kernel für ARM-Plattformen
13148	Mandrake	Schwachstellen im Linux-Kernel
13149	Mandrake	Schwachstelle in Sysklogd
13150	SGI	Linux-Sicherheitsupdate #19
13151	SGI	Linux-Kernel-Update #3
13165	Red Hat	Buffer Overflow in XChat
13166	Red Hat	Schwachstellen in LHA
13167	Red Hat	Speicherleck in Apache-Mod_ssl
13171	Debian	Schwachstelle in Eterm
13173	Debian	Schwachstellen in Midnight Commander »mc«
13174	Mandrake	Schwachstellen in Midnight Commander »mc«
13175	Mandrake	Schwachstelle in Libpng
13192	Red Hat	Schwachstelle in Libpng
13194	Debian	Race Condition in Flim
13195	Red Hat	Schwachstellen in Midnight Commander »mc«
13196	Debian	Schwachstelle in Libpng
13197	Debian	Schwachstelle in Rsync
13198	Mandrake	Schwachstelle in ProFTPD
13199	Red Hat	Schwachstelle in Utempter
13203	Red Hat	Schwachstelle in der Open-Office-Bibliothek Neon
13214	Suse	Mehrere Schwachstellen im Linux-Kernel
13227	Debian	Schwachstellen in mehreren Apache-Modulen
13249	Suse	Fehlkonfiguration der Suse-9.1-Live-CD
13253	Debian	Schwachstellen in Exim
13278	Red Hat	Überarbeitete OpenSSL-Pakete verfügbar
13288	Debian	Schwache Authentifizierung durch X-Server
13291	Mandrake	Schwachstelle in Rsync
13292	Mandrake	Schwachstelle in Apache-2-Mod_ssl
13305	Debian	Schwachstellen in Exim und Exim-TLS
13306	Red Hat	Schwachstellen im ISAKMP-Daemon
13307	Red Hat	Überarbeitete Kernelpakete

In Zusammenarbeit mit dem DFN-CERT

BEA Weblogic Server und Express

In BEA Weblogic Server und Express wurden mehrere Lücken entdeckt. Eventuell erhält eine Gruppe unerwartet Privilegien: Falls der Admin zwei Gruppen erzeugt, die erste zum Mitglied der Gruppe 2 ernennt, Gruppe 2 löscht und dann wieder erzeugt, wird Gruppe 1 überraschend Mitglied der neuen Gruppe 2 und erbt deren Rechte. Betroffen sind die Versionen 8.1 bis SP 2 und 7.0 bis SP 4. [http://www.securitytracker.com/alerts/2004/Apr/1009763.html]

Unter Umständen kann ein lokaler Angreifer das Datenbank-Passwort für JDBC erfahren. Es liegt als Klartext in »config.xml«. Betroffen sind die Versionen 8.1 bis SP 2, 7.0 bis SP 4 und 6.1 bis SP 6. [http://www.securitytracker.com/alerts/2004/Apr/1009764.html]

Wegen einer Schwachstelle bei SSL-Verbindungen kann sich ein entfernter Angreifer als ein anderer Client ausgeben. Betroffen sind Version 8.1 bis SP 2 und 7.0 bis SP 4. [http://www.securitytracker.com/alerts/2004/Apr/1009765.html]

Besitzt ein Angreifer das Recht, Programme auf dem Server zu installieren und auszuführen, dann ist er in der Lage, an fremde Benutzer-Accounts zu gelangen. Betroffen sind Versionen 8.1 bis SP 2 sowie 7.0 bis SP 4. [http://www.securitytracker.com/alerts/2004/Apr/1009766.html]

Ein Bug beim Verarbeiten von URLs gibt einem entfernten Angreifer Zugang zu gesperrten Adressen. Betroffen sind Version 7.0 SP4 und älter sowie 8.1 SP1 und älter. [http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_56.00.jsp]

Ein entfernter, angemeldeter User mit dem Recht, eigene Anwendungen zu schreiben, kann unberechtigt EBH-Objekte löschen. Betroffen sind die Versionen vor 8.1 SP2, 7.0 SP4 und 6.1 SP6. [http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_57.00.jsp]

Ein lokaler Angreifer kann durch Fehler in »config.sh« und »config.cmd« das Administrator-Passwort erfahren. Betroffen: Version 8.1 SP2 sowie jene vor 8.1. [http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA04_58.0 0.jsp] ■

Heimdal »k5admind«

Aufgrund eines Heap-Overflow-Fehlers in »k5admind« kann ein entfernter Angreifer Befehle mit den Rechten des Kerberos-Daemon ausführen. Der Overflow tritt vor der Authentifizierung im KDC-Interface auf (Key Distribution Center).

Nur Systeme mit Kerberos-4-Support sind betroffen, da sich der Bug in den Routinen für Kerberos 4 Compatibility Administration Requests befindet. Ein Angreifer kann ihn ausnutzen, indem er eine Nachricht mit einer Framing-Länge von weniger als 2 Byte sendet.

Betroffen sind die Versionen 0.6.1 und älter. [http://www.securityfocus.com/bid/10288] ■

Suse Linux

Ein Konfigurationsfehler auf der Live-CD der Suse Linux 9.1 Personal Edition gibt entfernten Angreifern Root-Zugriff. Die Live-CD vergibt kein Root-Passwort, startet aber einen SSH-Server. Ohne Authentifizierung kann sich jeder User als Root einloggen und etwa den Festplatteninhalt manipulieren. [http://www.securityfocus.com/bid/10297]

Einige Suse-Kernelversionen setzen auf die Proc-FS-Datei »/proc/scsi/qla2300/HbaApiNode« die falschen Rechte. Hierdurch kann ein lokaler Angreifer einen Denial-of-Service-Angriff ausführen. [http://www.securityfocus.com/bid/10279]

In Yast steckt eine Symlink-Schwachstelle. Beim Online-Update erzeugt Yast in »/usr/tmp/you-*Username*« mehrere temporäre Dateien: »cookies«, »quickcheack«, »yourservers«. Ein Angreifer kann vor dem Update passende symbolische Links ablegen. [http://www.securityfocus.com/bid/10047] ■

KAME Racoon

Ein Authentifizierungsfehler in Racoon, dem ISAKMP-Daemon des KAME-Projekts (IPsec-Authentifizierung und Schlüsseltausch), führt dazu, dass sich entfernte Angreifer mit gültigem Zertifikat trotz ungültigen Schlüssels anmelden können. Der Programmierfehler liegt in der Funktion »eay_check_x509sign()« (in »crypto_openssl.c«).

Betroffen sind die »crypto_openssl.c«-Dateiversion 1.83 sowie frühere. [http://www.securitytracker.com/alerts/2004/Apr/1009694.html]

Ein entfernter Angreifer kann Racoon abstürzen lassen und einen Denial of Service ausführen. Er muss ein ISAKMP-Paket mit speziell konstruiertem Header senden, Racoon hat dann Probleme bei der Speicherallokation. Betroffen sind die Versionen vor Racoon 20040408a. [http://www.securityfocus.com/bid/10172]. ■

Kurzmeldungen

Neon vor 0.24.5: Format-String-Fehler beim Verarbeiten von »XML/207«-Nachrichten, entfernter Angreifer kann Befehle mit den Rechten des Neon-Users ausführen. [http://www.securityfocus.com/bid/10136]

Helix Universal Server vor 9.0.3: Verarbeitungsfehler von HTTP-»GET«-Anfragen, entfernter Angreifer kann Server zum Absturz bringen. [http://www.securityfocus.com/bid/10157]

Realserver 8.02: Speichert Accountdaten als Klartext in »default.cfg«, lokaler Angreifer kann dieses File lesen. [http://www.securitytracker.com/alerts/2004/Apr/1009881.html]

Phorum 3.4.7: Eingabekontrollfehler im »include/userlogin.php«-Skript, SQL-Injection möglich. [http://www.securityfocus.com/bid/10173]

XChat 1.8.0 bis 2.0.8: Buffer Overflow in Socks-5-Proxy-Code, entfernter Angreifer kann Befehle mit den Rechten des XChat-Anwenders ausführen. [http://www.securityfocus.com/bid/10168]

Utempter: Eingabekontroll- und Symlink-Fehler beim Verarbeiten von Pfadangaben, lokaler Angreifer kann Dateien des Systems mit Root-Rechten überschreiben. [http://www.securitytracker.com/alerts/2004/Apr/1009870.html]

Ident2 1.04 (und älter): Buffer Overflow in »child_service()«, entfernter Angreifer kann Befehle mit Ident2-Rechten ausführen. [http://www.securitytracker.com/alerts/2004/Apr/1009912.html]

Tikiwiki 1.8.1 und älter: Zahlreiche Skripte sind anfällig für SQL-Injection und Cross-Site-Skripting; außerdem kann ein Angreifer Files hochladen und ausführen. [http://www.gulftech.org/04112004.php]

Advanced Guestbook 2.2: Fehler beim Verarbeiten des Passworts, SQL-Injection möglich. [http://www.securityfocus.com/bid/10209]

Artmedic HP-Maker: Double-Dot-Fehler in »index.php«-Skript, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/10207]

Protector System 1.15 b1: Eingabekontrollfehler bei URL-Verarbeitung, SQL-Injection möglich. [http://www.securityfocus.com/bid/10206]

Sysklogd 1.4.1 und 1.4.1-14: Fehler bei Speicherallokation, entfernter Angreifer kann »sysklogd« abstürzen lassen. [http://www.securitytracker.com/alerts/2004/Apr/1009976.html]

RSniff 1.0: Fehler beim Verarbeiten von Verbindungswünschen, entfernter Angreifer kann Denial of Service durchführen. [http://www.securityfocus.com/bid/10093]

Midnight Commander: Mehrere Buffer-Overflow- und Format-String-Fehler, lokaler Angreifer könnte Rechte des »mc«-Anwenders erhalten. [http://www.securitytracker.com/alerts/2004/Apr/1009981.html]

Libpng: Speicherzugriffsfehler bei Fehlermeldungen, entfernter Angreifer kann Libpng-Anwendungen durch geschickt konstruierte Bilddateien zum Absturz bringen. [http://www.securityfocus.com/bid/10244]

Gentoo Portage vor 2.0.50-r3: Symlink-Fehler, Denial of Service möglich. [http://www.securityfocus.com/bid/10060]

Linux-Kernel

Ein Buffer-Overflow in der Linux-Implementierung des ISO9660-Dateisystems führt dazu, dass ein lokaler Angreifer Befehle mit Kernel-Rechten ausführen kann. Er muss eine CD mounten, die manipulierte Symlinks enthält. Der Programmierfehler liegt in »rock_ridge_symlink_readpage()« und »get_symlink_chunk()«, beide in »fs/isofs/rock.c«. Betroffen sind die Versionen 2.4, 2.5 und 2.6. [http://www.securitytracker.com/alerts/2004/Apr/1009782.html]

Auch die Implementierungen von Ext 3, XFS und JFS sind fehlerhaft. Ein lokaler Angreifer ist in der Lage, Bereiche des Systemspeichers auszulesen. Betroffen davon sind die 2.4-Versionen bis 25 sowie die 2.6er bis 5. [http://www.securitytracker.com/alerts/2004/Apr/1009797.html], [.../1009798.html] und [.../1009799.html]

Ein weiteres Sicherheitsleck findet sich im Soundblaster-Treiber. Ein lokaler Angreifer kann das System zum Absturz bringen. Betroffen sind die Versionen 2.4.25 und älter sowie 2.6.5 und älter. [http://www.securitytracker.com/alerts/2004/Apr/1009800.html]

Durch einen Integer-Overflow im »setsockopt()«-Syscall kann ein lokaler Angreifer Root-Rechte erlangen. Der Code in »net/ipv4/ip_sockglue.c« verarbeitet die Option »IP_MSFILTER_SIZE« nicht korrekt. Betroffen sind die Kernelversionen 2.4.22 bis 2.4.25 und 2.6.1 bis 2.6.3. [http://isec.pl/vulnerabilities/isec-0015-msfilter.txt]

Ein Vorzeichenfehler im Proc-Handler »cpufreq_userspace« führt dazu, dass ein lokaler Angreifer Kernel-Speicherbereiche lesen kann. Der Fehler liegt in »drivers/cpufreq/cpufreq_userspace.c«. Betroffen sind Kernel der Versionen 2.4, 2.5 und 2.6. [http://www.securitytracker.com/alerts/2004/Apr/1009924.html]

Ein Buffer-Overflow-Fehler wurde in der »panic()«-Funktion gefunden. Das Advisory nennt keine konkreten Auswirkungen. Betroffen davon sind Kernel 2.4 und 2.6. [http://www.securitytracker.com/alerts/2004/Apr/1009931.html]

Ein Fehler in der Funktion »fb_copy_cmap()« im Framebuffer-Treiber hat ebenfalls unbekannte Auswirkungen. Betroffen ist Kernel 2.6. [http://www.securitytracker.com/alerts/2004/Apr/1009961.html]

Ein Programmierfehler in der »do_fork()«-Funktion gibt lokalen Angreifern die Chance, eine Denial-of-Service-Attacke durchzuführen. Betroffen sind 2.4er und 2.6er Kernel. [http://www.securitytracker.com/alerts/2004/Apr/1009990.html] ■

Apache-Webserver

Durch einen Buffer Overflow in Apache kann ein entfernter Angreifer Befehle mit Webserver-Rechten ausführen – vorausgesetzt der Server läuft auf keinem 32-Bit-System. Der Bug steckt in der »ebcdic2ascii()«-Funktion.

Sie kopiert einen 64-Bit-Wert in eine zu klein gewählte Variable. Der Fehler findet sich unter anderem in Mod_auth, Mod_auth3 und Mod_auth4. Betroffen sind die Versionen 1.3.29 und älter. [http://www.securitytracker.com/alerts/2004/Apr/1009934.html] *(M. Vogelsberger/fjl)* ■

Kurzmeldungen

Coppermine Photo Gallery 1.2.2b und 1.2.0 RC4: Mehrere Eingabekontrollfehler, entfernter Angreifer kann eigene Befehle einschleusen. [http://www.securitytracker.com/alerts/2004/Apr/1010001.html]

Flim Emacs-Library 1.14.6: Symlink-Bug beim Anlegen temporärer Dateien, lokaler Angreifer kann Dateien mit den Rechten des Emacs-Anwenders überschreiben. [http://www.securityfocus.com/bid/10259]

Pound 1.5 und älter: Format-String-Fehler beim Logging, entfernter Angreifer kann Befehle mit den Rechten des Pound-Daemon ausführen. [http://www.securitytracker.com/alerts/2004/May/1010034.html]

IP-Menu 0.0.3: Symlink-Fehler beim Anlegen von temporären Dateien, lokaler Angreifer kann Dateien mit Root-Rechten überschreiben. [http://www.securityfocus.com/bid/10269]

P4DB 2.01 (und älter): Verschiedene Eingabekontrollfehler, Cross-Site-Skripting möglich; entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/10286]

Delegate 8.9.2 (und älter): Buffer Overflow in SSLway-Filter, entfernter Angreifer kann Befehle mit den Rechten des Delegate-Prozesses ausführen. [http://0xbadc0ded.org/advisories/0401.txt]

Kolab vor 1.0-20040426: Die Datei »/var/origkolab/etc/openldap/slapd.conf« ist für alle lesbar, lokaler Angreifer kann OpenLDAP-Server-Passwort erfahren. [http://www.securityfocus.com/bid/10277]

Tutos 1.1.20031017: Einige Eingabekontrollfehler in mehreren PHP-Skripten, Cross-Site-Skripting und SQL-Injection möglich; entfernter Angreifer kann an sicherheitsrelevante Informationen gelangen. [http://www.securitytracker.com/alerts/2004/Apr/1009750.html]

MySQL 4.0.18, 3.23.58: Symlink-Schwachstelle in Mysqld_multi beim Anlegen von »/tmp/mysqld_multi.log«, lokaler Angreifer kann Dateien mit den Rechten des »mysqld_multi«-Anwenders überschreiben. [http://www.securityfocus.com/bid/10142]

Cisco IPsec-VPN-Client: Unsichere Aufbewahrung des IPsec-Gruppenpasswords, lokaler Angreifer kann IPsec-Passwort lesen. [http://www.securityfocus.com/bid/10155]

PHP-Bugtracker 0.9.1: Verschiedene Eingabekontrollfehler unter anderem bei »bug_id«-Variable; SQL-Injection und Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Apr/1009821.html]

Logcheck 1.1.1: Symlink-Schwachstelle beim Anlegen von temporären Dateien in »/var/tmp«, lokaler Angreifer kann Dateien mit Root-Rechten überschreiben. [http://www.securityfocus.com/bid/10162]

Rsync 2.6.1 (und älter): Fehler beim Verarbeiten von Pfadangaben, entfernter Angreifer kann Daten außerhalb des Modulpfads speichern. [http://www.securityfocus.com/bid/10247]

Veritas Net-Backup: Buffer-Overflow- und Format-String-Fehler, entfernter Angreifer kann eventuell Befehle mit Root-Rechten ausführen. [http://www.securitytracker.com/alerts/2004/Apr/1010011.html]

Surge-LDAP 1.0g: Double-Dot-Fehler im »user.cgi«-Skript, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.securitytracker.com/alerts/2004/Apr/1009732.html]

Gnome Nautilus 2.2.1: Fehler bei Verzeichnisnamen mit über 255 Zeichen, Angreifer kann einen Denial of Service ausführen. [http://www.securitytracker.com/alerts/2004/Apr/1009738.html]

LHA: Buffer Overflow, entfernter Angreifer kann Befehle mit den Rechten des LHA-Anwenders ausführen; Fehler beim Verarbeiten von Pfadangaben in gepackten Dateien, entfernter Angreifer kann Dateien mit den Rechten des LHA-Anwenders überschreiben oder neu anlegen. [http://www.securityfocus.com/bid/10243]

ProFTPD 1.2.9: Fehler in ACLs (Access Control List) mit CIDR-basierten Adressen; entfernter, angemeldeter Angreifer erhält unberechtigt Zugriff auf Dateien. [http://www.securityfocus.com/bid/10252]

Checkpoint VPN-1 NG, VSX und GX: Buffer Overflow beim Verarbeiten von ISAKMP-Paketen, entfernter Angreifer kann Befehle einschleusen. [http://www.securitytracker.com/alerts/2004/May/1010058.html]

Monit bis 4.2 und bis 4.3 Beta 2: Buffer Overflow im Administrationsinterface, entfernter Angreifer kann Befehle als Root einschleusen. [http://www.securityfocus.com/bid/10051]