InSecurity News

KDE-PIM

Ein Buffer-Overflow in der KDE-PIM-Komponente führt dazu, dass entfernte und lokale Angreifer Befehle mit den Rechten des KDE-PIM-Anwenders ausführen können. Der Overflow tritt beim Lesen von VCF-Dateien auf. Ein Angreifer muss nur ein geschickt konstruiertes VCF-File an sein Opfer senden und hoffen, dass es sie mit KDE-PIM öffnet – in der Standardkonfiguration liest das Programm nur lokale Dateien. Betroffen von diesem Problem sind die KDE-Versionen 3.1.0 bis 3.1.4. [http://www.securitytracker.com/alerts/2004/Jan/1008715.html] ■

PHP-Groupware

In PHP-Groupware wurden einige sicherheitsrelevante Schwachstellen entdeckt. Die »calendar«- und »infolog«-Module verarbeiten Benutzereingaben nicht korrekt. Dadurch kann ein entfernter Angreifer SQL-Injection-Attacken erfolgreich ausführen. Aufgrund einer weiteren Sicherheitslücke im »calendar«-Modul kann ein Benutzer Holiday-Dateien mit eingebettetem PHP-Code auf das System laden und seine Routinen später ausführen.
Betroffen sind die Versionen vor 0.9.14.007. [http://www.securitytracker.com/alerts/2004/Jan/1008662.html] ■

Suse Linux

Suse Linux 9.0 enthält zahlreiche Skripte mit Symlink-Fehlern. Dazu gehören unter »/usr/X11R6/bin« die Skripte »fvwm-bug«, »wm-oldmenu-2new«, »x11perfcomp« und »xf86debug« sowie »/opt/kde3/bin/winpopup-send.sh« und »/sbin/lvmcreate_initrd«. Sie legen temporäre Files mit leicht zu erratenden Namen an.
Ein lokaler Angreifer kann die Sicherheitslücken ausnutzen, um fremde Files zu manipulieren. Er erhält dabei die Rechte des Users, der die Skripte ausführt. [http://www.securitytracker.com/alerts/2004/Jan/1008781.html]
Zudem enthält das Konfigurationsprogramm »3ddiag« eine Symlink-Schwachstelle. Mehrere Skripte, die zu diesem Tool gehören, benutzen temporäre Dateien unsicher. Lokale Angreifer können fremde Files überschreiben, sie erhalten dabei die Rechte des »3ddiag«-Users. [http://www.securitytracker.com/alerts/2004/Jan/1008804.html]
Ein weiterer Symlink-Fehler tritt in »SuSEconfig.gnome-filesystem« auf. Er erlaubt, dass lokale Angreifer Dateien mit Root-Rechten überschreiben können. [http://www.securitytracker.com/alerts/2004/Jan/1008703.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	Forum: [http://forums.gentoo.org/] Liste: [http://www.gentoo.org/main/en/lists.xml] (gentoo-announce und gentoo-security) Betreff: GLSA: ... [1]	Gentoo bietet leider keine Webseite zu Sicherheitsaktualisierungen und anderen Security-Informationen. Als Ersatz dient das Forum. In dessen Rubrik »News and Announcements« sind dann auch die Advisories zu finden.
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/errata/] Liste: [http://www.redhat.com/mailing-lists/] (redhat-watch-list) Betreff: [RHSA-... [1]	Red Hat sortiert die Security Advisories bei den so genannten Errata ein: Zu jeder Red-Hat-Linux-Version sind dort alle bekannt gewordenen Fehler beschrieben. Die Security Advisories liegen als HTML-Seite vor, mit Links zu den Patches.
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.	

Macromedia Coldfusion

Durch einen Fehler in Macromedia Coldfusion kann ein Java-Objekt die Sicherheitsrestriktionen der Sandbox umgehen. Ein angemeldeter entfernter Angreifer kann so sicherheitskritische Befehle ausführen. Anfällig sind die Versionen MX 6.1 Enterprise und MX 6.1 J2EE. [http://www.securitytracker.com/alerts/2004/Jan/1008877.html]

Ein weiteres Problem tritt auf, wenn Coldfusion Form-Felder verarbeitet. Eine hohe Anzahl solcher Felder führt dazu, dass Coldfusion sehr viel Zeit für das Verarbeiten benötigt. Betroffen sind die Versionen MX 6.1 (alle Editionen) und MX 6.1 J2EE (alle Editionen). [http://www.securitytracker.com/alerts/2004/Jan/1008878.html] ■

Tabelle 2: Linux-Advisories vom 16.01. bis 14.02.04

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

ID	Linux	Beschreibung
11754	Debian	Schwachstelle im Linux-Kernel (Mips und Mipsel)
11755	Debian	Schwachstelle in Netpbm-free
11758	Debian	Schwachstellen in Tcpdump
11759	Debian	Schwachstelle im Midnight Commander (»mc«)
11785	Debian	Buffer Overflow in Slocate
11788	Red Hat	Schwachstelle in »mc«
11825	Red Hat	Buffer Overflow in Slocate
11853	Mandrake	Schwachstelle in Slocate
11854	Mandrake	Schwachstelle in Jabber
11872	Red Hat	Schwachstellen in Gaim
11879	Debian	Schwachstelle in GnuPG
11880	Mandrake	Schwachstellen in Tcpdump
11881	Mandrake	Schwachstelle in Gaim
11882	Mandrake	Schwachstelle in »mc«
11917	Debian	Schwachstelle in »trr19«
11918	Suse	Schwachstellen in Gaim
11946	Debian	Schwachstelle in Suidperl
11947	Mandrake	Update zur Schwachstelle in Gaim
11994	Debian	Buffer Overflow in Crawl
11995	Debian	Lokale Schwachstelle im Linux-Kernel 2.4 (Mips)
12000	Mandrake	Neue Glibc-Pakete erhältlich
12001	Red Hat	Schwachstellen im Kernel, in Util-Linux und »mc«
12005	Generisch	Schwachstellen in der H.323-Implementierung der Checkpoint FW-1
12006	Generisch	Format-String-Schwachstellen in Checkpoint Firewall-1 HTTP-Parser
12007	Generisch	Schwachstellen in Checkpoint-ISAKMP-Verarbeitung
12008	Red Hat	Cross-Site-Skripting-Schwachstellen in Mailman
12009	Red Hat	Race Conditions in Netpbm
12010	Generisch	Schwachstelle im GNU-Radius-Server
12015	Debian	Schwachstellen in Gaim
12052	Debian	Heap Overflow in Mpg123
12054	Debian	Mehrere Schwachstellen in Mailman
12091	Red Hat	Neue Mutt-Pakete verfügbar
12106	Mandrake	Schwachstelle in Mutt
12108	Mandrake	Schwachstellen in Netpbm
12124	Red Hat	Schwachstellen in XFree86
12125	Red Hat	Schwachstellen in PWLib

In Zusammenarbeit mit dem DFN-CERT

»nd«

Gleich mehrere Buffer-Overflow-Fehler in dem WebDAV-Client »nd« führen dazu, dass ein entfernter Angreifer Befehle mit den Rechten des »nd«-Anwenders ausführen kann. Er benötigt dazu Kontrolle über einen WebDAV-Server. Die Overflows treten beispielsweise auf, wenn der Server überlange URLs, Lock-Token oder Authentication-Realm-Strings sendet.

Betroffen sind die Versionen 0.8.1 und älter. [http://www.securitytracker.com/alerts/2004/Jan/1008616.html] ■

V-Box

Ein Programmierfehler in V-Box (Anrufbeantworter für ISDN) erlaubt, dass ein lokaler Angreifer Befehle mit Root-Rechten ausführen kann. Der Code in »vboxgetty/voice.c« gibt die Root-Rechte nicht ab, bevor er ein benutzerdefiniertes Tcl-Skript startet. Besondere Tricks muss der Angreifer nicht kennen – V-Box führt sein komplettes Skript als Root aus.

Betroffen hiervon sind die V-Box-Versionen 0.1.7 und älter. [http://www.securityfocus.com/bid/9381] ■

Phorum

Das Phorum-Skript »register.php« verarbeitet die Variable »hide_email« nicht korrekt. Dadurch kann ein entfernter Angreifer SQL-Kommandos in die Datenbank einschleusen. Ein weiterer Programmierfehler in der Funktion »phorum_check_xss()« (in »common.php«) erlaubt es einem entfernten Angreifer, Cross-Site-Skripting-Attacken durchzuführen. Die gleiche Konsequenz haben auch Fehler in den beiden Dateien »profile.php« (»EditError«-Variable) und »login.php« (»Error«-Variable).

Anfällig sind die Versionen 3.4.5 und älter. [http://www.securitytracker.com/alerts/2004/Jan/1008633.html] ■

Tcpdump

In Tcpdump 3.8.1 wurden drei Fehler entdeckt, die beim Analysieren einiger Protokolle auftreten. Ein Angreifer kann den Sniffer zum Absturz bringen. Der erste Bug betrifft Radius-Pakete: Die Funktion »print_attr_string()« (in »print-radius.c«) prüft die Variablen »length« und »data« nicht korrekt. [http://www.securitytracker.com/alerts/2004/Jan/1008735.html]

Den zweiten Fehler lösen ISAKMP-Pakete aus. Er verbirgt sich in der »rawprint()«-Funktion (»print-isakmp. c«). [http://www.securitytracker.com/alerts/2004/Jan/1008716.html]

Beim Handling von L2TP-Paketen tritt ein weiteres Problem auf. Fehlerhaft ist die Funktion »l2tp_avp_print()« (»print-l2tp.c«). [http://www.securitytracker.com/alerts/2004/Jan/1008748.html] ■

H+BEDV Antivir

Durch eine Schwachstelle in der Linux-Version des Virenscanners H+BEDV Antivir kann ein lokaler Angreifer Dateien mit Root-Rechten überschreiben. Es handelt sich um eine typische Symlink-Schwachstelle.

Antivir achtet beim Erzeugen temporärer Dateien im Verzeichnis »/tmp« nicht darauf, ob die anzulegende Datei schon vorhanden ist. Der Name, den Antivir verwendet, ist sehr einfach zu erraten: »/tmp/.pid_antivir_*PID*«. Betroffen ist die Antivir-Version 2.0.9-9. [http://www.securityfocus.com/bid/9413] ■

Apache-Module

Ein Fehler in Mod_auth_shadow (ein Authentifizierungsmodul für Apache) führt dazu, dass sich Benutzer mit abgelaufenen Passwörtern immer noch anmelden können. Betroffen sind die Versionen vor 1.4. [http://www.securitytracker.com/alerts/2004/Jan/1008675.html]

Ein weiteres Problem im Mod_perl-Modul erlaubt es entfernten Angreifern, HTTP- und HTTPS-Verbindung zu übernehmen (Session Hijacking). Der Fehler entsteht durch einen unsauberen Umgang mit Dateideskriptoren in Mod_perl. Betroffen ist Version 1.99_09. [http://www.securitytracker.com/alerts/2004/Jan/1008822.html]

Eine Sicherheitslücke in Mod_python führt dazu, dass ein entfernter Angreifer den Apache-Webserver zum Absturz bringen kann. Anfällig ist die Version 2.7.9. [http://www.securitytracker.com/alerts/2004/Jan/1008828.html]

Das Mod_digest-Modul ist ebenfalls fehlerhaft. Ein entfernter Angreifer kann sich unberechtigt am System anmelden. Betroffen sind die Version 1.3.29 und älter. [http://www.securitytracker.com/alerts/2004/Feb/1008920.html] ■

Lotus Domino

Durch einen Konfigurationsfehler in Lotus Domino kann ein lokaler Angreifer sicherheitsrelevante Konfigurationsdateien ändern. Lotus installiert die Files »/local/notesdata/notes.ini« und »/opt/lotus/LPSilent.ini« global beschreibbar. Durch Eingriffe in »notes.ini« kann ein Angreifer Schlüsseleinträge manipulieren. Eine Übersicht aller verfügbaren Schlüsseleinträge inklusive Erklärung steht bei: [http://www.drcc.com/A55711/ref/notesini.nsf]

Betroffen hiervon ist die Version 6.0.2. [http://www.securityfocus.com/bid/9366] ■

Kurzmeldungen

Aiptek Netcam-Webserver 1.0.0.28 (und älter): Double-Dot-Fehler beim Verarbeiten von URLs, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/9456]

Vsftpd 1.1.3: Antwortverhalten bei gültigen Benutzernamen anders als bei ungültigen Namen, entfernter Angreifer kann herausfinden, ob ein bestimmter Benutzername auf dem System existiert. [http://www.securitytracker.com/alerts/2004/Jan/1008628.html]

Postnuke 0.726: Eingabekontrollfehler in den Modulen »download« und »mebers_list«, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Jan/1008629.html]

FSP 2.8.1b17 (und älter): Buffer Overflow und Eingabekontrollfehler in »validate_path()«-Funktion, entfernter Angreifer kann Befehle ausführen und auf Dateien außerhalb des FSP-Rootverzeichnisses zugreifen. [http://www.securityfocus.com/bid/9377]

Metadot Portal Server bis 5.6.5.4b5: Fehlerhafte Eingabekontrolle der »id«- und »key«-Variablen, SQL-Injection und Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Jan/1008747.html]

PHP vor 4.3.2: Fehlerhafte Eingabefilterung der »PHPSESSID«-Variable, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Jan/1008653.html]

Helix Universal Server: Fehler beim Verarbeiten von HTTP-»POST«-Nachrichten auf dem Administrator-Port, entfernter Angreifer kann Denial-of-Service-Attacken durchführen. [http://www.securitytracker.com/alerts/2004/Jan/1008701.html]

YABB SE 1.5.4, 1.5.3 (eventuell andere): Eingabekontrollfehler in »SSI.php« bei »ID_MEMBER«-Variable, SQL-Injection möglich. [http://www.securityfocus.com/bid/9449]

Q-Mail 1.03: Buffer Overflow bei SMTP-Handling, entfernter Angreifer kann eventuell eigene Befehle einschleusen. [http://www.securitytracker.com/alerts/2004/Jan/1008733.html]

N-Cipher Payshield 1.3.12, 1.5.18 und 1.6.18: Fehlerhafter Rückgabewert einer Verifikationsfunktion, Anwendungen, die diese Bibliothek nutzen, machen Fehler bei der Authentifizierung. [http://www.securitytracker.com/alerts/2004/Jan/1008710.html]

PHP-Dig 1.6.5: Datei-Include-Fehler in »config.php«, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/9424]

Fishcart 3.0 (und älter): Integer Overflow bei zu großer Zahl bestellter Waren, entfernter Angreifer kann das System so manipulieren, dass negative Beträge auf der Gesamtrechnung erscheinen. [http://www.securityfocus.com/bid/9426]

Jitterbug 1.6.2: Fehlerhafte Eingabefilterung, entfernter Angreifer kann Befehle einschleusen. [http://www.securityfocus.com/bid/9397]

Simpledata vor 4.0.3: Authentifizierungsproblem, entfernter Angreifer kann Zugriff erlangen. [http://www.securityfocus.com/bid/9380]

OpenCA vor 0.9.1.7: Fehler in »crypto-utils.lib«, das System vertraut Signaturen, die nicht vertrauenswürdig sind. [http://www.securitytracker.com/alerts/2004/Jan/1008744.html]

Netpbm 10.19 (und älter): Zahlreiche Symlink-Schwachstellen, lokaler Angreifer kann Dateien mit Rechten des Netpbm-Benutzers überschreiben. [http://www.securitytracker.com/alerts/2004/Jan/1008757.html]

Bugs vor 1.2: Das Skript »bugs/userbase_connect.inc« ist direkt aufrufbar, entfernter Angreifer kann Datenbank-Authentifizierungsdaten sehen. [http://www.securitytracker.com/alerts/2004/Jan/1008758.html]

Legato Networker 6.0: Symlink-Fehler im »nsr_shutdown«-Skript, lokaler Angreifer kann Dateien mit Root-Rechten überschreiben. [http://www.securityfocus.com/bid/9446]

Web Crossing 4.x, 5.x: Fehler beim Verarbeiten großer »Content-Length«-Werte bei HTTP-»POST«-Anfrage, entfernter Angreifer kann Server zum Absturz bringen. [http://www.securitytracker.com/alerts/2004/Feb/1008927.html]

IBM Cloudscape 5.1: Schlechte Standardkonfiguration und Fehler in »sun.*«- und »org.apache.*«-Paketen, entfernter Angreifer kann Befehle einschleusen. [http://www.securitytracker.com/alerts/2004/Feb/1008952.html]

IBM Net.Data 7 und 7.2: Eingabekontrollfehler in »db2www«-CGI-Programm, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9488]

Linux-Kernel

Mehrere Schwachstellen wurden im Linux-Kernel gefunden. Ein Fehler steckt in der »do_mremap()«-Funktion. Sie überprüft eine Benutzerangabe nicht korrekt. Als Folge kann ein lokaler Angreifer virtuelle Speicherbereiche der Größe 0 anlegen und so die Speicherverwaltung verwirren. Über Umwege erlangt er Root-Rechte. Betroffen von diesem Problem sind die Kernelversionen 2.4 und 2.6. [http://isec.pl/vulnerabilities/isec-0013-mremap.txt]

Eine weitere Schwachstelle hat der 2.4er Kernel. Durch einen Programmierfehler in den Realtime-Clock-Routinen kann ein lokaler Angreifer Speicherbereiche des Kernels einsehen und unter Umständen an Sicherheits-Informationen gelangen. [http://www.securitytracker.com/alerts/2004/Jan/1008594.html]

Der Linux-Kernel 2.4.21 für AMD64-Systeme begeht einen Fehler beim Behandeln der »eflags«. Damit können lokale Angreifer höhere Rechte erlangen, eventuell sogar Root-Rechte. [http://www.securitytracker.com/alerts/2004/Jan/1008775.html]

Ein weiteres Problem wurde im R128-DRI-Treiber gefunden. Auch damit kann ein lokaler Angreifer höhere Rechte auf dem System erlangen. Betroffen sind die Kernelversionen vor 2.4.22. [http://www.securitytracker.com/alerts/2004/Feb/1008921.html]

Der C-Media-PCI-Sound-Treiber ist von einer weiteren Schwachstelle betroffen. Sie erlaubt es lokalen Angreifern, auf Speicherbereiche fremder Prozesse zuzugreifen. Betroffen hiervon sind Kernel vor Version 2.4.22. [http://www.securitytracker.com/alerts/2004/Feb/1008935.html]

Schwerer wiegende Konsequenzen hat ein Buffer Overflow in dem IXJ-Telephony-Card-Treiber. Durch ihn kann ein lokaler Angreifer unter Umständen Root-Rechte auf dem System erlangen. Betroffen sind die Kernelversionen vor 2.4.20. [http://www.securitytracker.com/alerts/2004/Feb/1008937.html] ■

INN

Ein Buffer Overflow im Internet-Newsserver INN erlaubt es entfernten Angreifern, Befehle mit den Rechten des »innd«-Prozesses auszuführen. Der Programmierfehler tritt in der »ARTpost()«-Funktion auf (»art.c«). Es handelt sich um ein Problem beim Handling von Kontrollnachrichten.

Zu dem Fehler kam es erst in der Version 2.4.0. [http://www.securityfocus.com/bid/9382] ■

Elm

Ein entfernter Angreifer kann eine E-Mail so geschickt konstruieren, dass sie beim Lesen mit Elm beliebige Befehle ausführt. Das ist möglich, weil Elm einen Buffer-Overflow-Fehler enthält, der beim »frm«-Befehl auftritt. Er kann durch einen überlangen E-Mail-Header hervorgerufen werden. Die Befehle laufen mit den Rechten des Elm-Anwenders. [http://www.securityfocus.com/bid/9430] ■

Kurzmeldungen

PHP-Nuke bis 6.9: Zahlreiche Eingabekontrollfehler, SQL-Injection möglich. [http://www.securitytracker.com/alerts/2004/Feb/1008897.html]

Xoops 2.x: Eingabekontrollfehler in »newbb«-Modul, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Jan/1008849.html]

I-Search: Datei-Include-Fehler in »isearch.inc.php«, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securitytracker.com/alerts/2004/Feb/1008900.html]

Util-Linux: Fehler im Login-Programm, lokaler Angreifer kann unter Umständen fremde Anmeldedaten einsehen. [http://www.securityfocus.com/bid/9558]

PHP-Myadmin 2.5.5-pl (und älter): Double-Dot-Fehler in »export.php«, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/9564]

PHP-Nuke-Modul GBook 1.0: Eingabekontrollfehler in den Feldern »name«, »email«, »city« und »message«, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9559]

Tunez vor 1.20-pre1: Eingabekontrollfehler in zahlreichen Skripten, SQL-Injection möglich. [http://www.securityfocus.com/bid/9565]

Reviewpost PHP Pro: Eingabekontrollfehler in »showproduct.php«- und »showcat.php«-Skripten, SQL-Injection möglich. [http://www.securityfocus.com/bid/9574]

Rx-Google 1.0: Eingabekontrollfehler in »rxgoogle.cgi«, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9575]

Mailman vor 2.1.3: Eingabekontrollfehler im »create«-Skript, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Feb/1008956.html]

Hotnews 0.7.2 und älter: Datei-Include-Fehler in »hotnews-engine.inc.php3«, entfernter Angreifer kann eigenen PHP-Code auf dem System ausführen. [http://www.securityfocus.com/bid/9357]

Postnuke-Modul Postcalendar 4.0.0: Eingabekontrollfehler in der Suchfunktion, SQL-Injection möglich. [http://www.securitytracker.com/alerts/2004/Jan/1008621.html]

Leafnode Fetchnews 1.9.47 und älter: Fehler beim Verarbeiten ungültiger News, entfernter Angreifer kann den Client dazu bringen, die Arbeit zu verweigern. [http://www.securityfocus.com/bid/8541]

EZ-Contents: Datei-Include-Fehler beim Verarbeiten der »link«-Variable, entfernter Angreifer kann eigenen Code einschleusen. [http://www.securityfocus.com/bid/9396]

Mambo Open Source 4.6: Datei-Include-Fehler in »mod_mainmenu.php« sowie Fehler beim Filtern der »itemid«-Variablen, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen, außerdem ist Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Jan/1008954.html] und [.../Feb/1008954.html]

Go-Ahead-Webserver 2.1.8: Eingabekontrollfehler sowie Problem beim Verarbeiten bestimmter HTTP-»POST«-Anfragen, entfernter Angreifer kann eigentlich nicht zugängliche Verzeichnisse erreichen und außerdem dafür sorgen, dass der Serverprozess die CPU völlig auslastet. [http://www.securitytracker.com/alerts/2004/Jan/1008760.html] und [.../1008766.html]

PHP-Shop 0.6.1-b: Mehrere Fehler beim Filtern von Benutzereingaben, SQL-Injection und Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Jan/1008746.html]

Mephistoles Httpd 0.6.0 final: Fehler beim Filtern von Benutzereingaben (URLs), Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9470]

Mpg321: Format-String-Fehler in »mpg321.c«, lokale und entfernte Angreifer können mit einer manipulierten MP3-Datei eigene Befehle einschleusen. [http://www.securityfocus.com/bid/9364]

Gaim 0.75 und älter: Zwölf Stack, Heap und Integer Overflows, ein entfernter Angreifer kann Befehle mit den Rechten des Gaim-Anwenders ausführen. [http://security.e-matters.de/advisories/012004.html]

GNU Radius

Ein Fehler in GNU Radius erlaubt es einem entfernten Angreifer, den Server abzuschießen. Das Problem tritt bei UDP-Datenpaketen auf, in denen nur das Attribut »Acct-Status-Type« gesetzt ist. Die Software liest dann von einem Null-Pointer und stürzt ab. Betroffen ist die Version 1.0. [http://www.securityfocus.com/bid/9578] ■

Honeyd

Honeyd sollte als Honeypot-System von einem etwaigen Angreifer nicht als solches erkannt werden. TCP-Pakete mit gesetzten SYN- und RST-Flags entlarven es jedoch. Der Fehler steckt in den Routinen, die typische Nmap-Fingerprints bearbeiten.
Die Schwachstelle betrifft alle Versionen vor 0.8. [http://www.securityfocus.com/bid/9464] ■

IBM Informix Dynamic Server

Der IBM Informix Dynamic Server hat mehrere Sicherheitslücken. In einigen Teilprogrammen führt die Umgebungsvariable »GL_PATH« zum Buffer Overflow. Das Programm »ontape« lässt sich mit der »ONCONFIG«-Variablen zum Overflow bringen. Weitere Tools sind anfällig für Format-String-Fehler.

Allen Lücken gemeinsam ist, dass sie es einem lokalen Angreifer erlauben, Befehle mit den Informix-Gruppenrechten oder gar mit Root-Rechten auszuführen.
Betroffen von dem Problem sind die Versionen 9.40.UC1 und 9.40.UC2. [http://www.securitytracker.com/alerts/2004/Jan/1008873.html] ■

Checkpoint Firewall-1 und VPN-1

In Checkpoint Firewall-1 und VPN-1 entdeckte das NISCC (UK National Infrastructure Security Co-Ordination Centre) mehrere Schwachpunkte, die bei der Verarbeitung von H.323-Nachrichten aufgetreten sind [http://www.uniras.gov.uk/vuls/2004/006489/h323.htm]. Zum Testen verwendete das NISCC die Programme der Oulu Security Programming Group [http://www.ee.oulu.fi/research/ouspg/]. Checkpoint bestätigte die Schwachstelle kurze Zeit später. [http://www.checkpoint.com/techsupport/alerts/h323.html]

Mehrere Format-String-Fehler stecken in der HTTP-AI-Komponente (Application Intelligence). Ein entfernter Angreifer kann sie ausnutzen, um auf dem Firewall-Rechner Befehle mit Root-Rechten auszuführen. [http://www.securitytracker.com/alerts/2004/Feb/1008947.html]
Ein Buffer Overflow in VPN-1 sowie in Securemote und Secureclient beim Verarbeiten von ISAKMP-Datenpaketen gibt einem entfernten Angreifer Root-Rechte. [http://www.securitytracker.com/alerts/2004/Feb/1008948.html] ■

BEA Weblogic Server und Express

In BEA Weblogic Server und Express wurden einige Probleme gefunden. Ein entfernter Angreifer kann per HTTP-»TRACE«-Anfrage Cross-Site-Skripting ausführen. [http://www.securitytracker.com/alerts/2004/Jan/1008866.html]
Durch einen zweiten Fehler kommen Operatoren zu Administrator-Rechten. Sie erhalten Zugriff auf sicherheitsrelevante MBean-Attribute, so zum Beispiel »ServerStartMBean.Password« und »NodeManagerMBean.CertificatePassword«. Betroffen ist die Version 8.1 (auch SP 1). [http://www.securitytracker.com/alerts/2004/Jan/1008867.html]

Auch für lokale Angreifer ist das Admin-Passwort erreichbar, es steht als Klartext in »config.xml«. [http://www.securitytracker.com/alerts/2004/Jan/1008868.html]
Eine ähnliches Problem betrifft die Accountdaten anderer Benutzer. [http://www.securitytracker.com/alerts/2004/Jan/1008869.html]
Durch Fehler in den Ant-Tasks »wldeploy«, »wlserver« und »wlconfig« kann ein lokaler Angreifer an das Admin-Passwort gelangen. Betroffen sind die Versionen 8.1 (SP 1) und älter. [http://www.securitytracker.com/alerts/2004/Jan/1008682.html] ■

Realplayer und Real One

In Realplayer und Real-One-Player wurden mehrere Buffer-Overflow-Schwachstellen gefunden. Ein entfernter Angreifer kann durch sie Befehle mit den Rechten des Real-Anwenders ausführen. Das Problem tritt auf, wenn der Player bestimmte ».RP«-, ».RT«-, ».RAM«-, ».RMP«- und ».SML«-Dateien über eine HTML-Referenz lädt.
Anfällig für das Problem ist die Version 8. [http://www.securitytracker.com/alerts/2004/Feb/1008946.html] ■

Neue Releases

4G8: Ein Paketsniffer für geswitchte Netzwerke. [http://forgate.sourceforge.net]

Env_audit: Programm zum Auditing des Prozess-Environments (etwa Umgebungsvariablen und Dateideskriptoren). [http://www.web-insights.net/env_audit/]

Yin-Yang: Kernelmodul zum Überwachen von Dateizugriffen. Übergibt jede Open-Operation an einen Daemon und öffnet die Datei erst, wenn der Daemon dies erlaubt. [http://yinyang.sourceforge.net]

Jabberd

Ein entfernter Angreifer kann eine Denial-of-Service-Attacke gegen den Jabber-Dienst durchführen und den Daemon »jabberd« zum Absturz bringen. Das Problem tritt bei SSL-Verbindungen auf. Der Programmierfehler liegt in der »mio_ssl.c«-Datei. Betroffen davon ist die Version 1.4.3. [http://www.securitytracker.com/alerts/2004/Jan/1008625.html]
(M. Vogelsberger/fjl) ■