InSecurity News

Open Office

Durch einen Fehler in Open Office kann ein lokaler Angreifer Zugriff auf Dokumente anderer Benutzer erlangen. Beim Start erzeugt die Office-Software – je nach Umask des Users – ein global lesbares, temporäres Verzeichnis mit Namen »/tmp/sv*Zufallszahl*.tmp«. Speichert ein Anwender eine Datei, so wandert eine gezippte Variante des Dokuments in dieses temporäre Verzeichnis. Auf diese Weise kann ein Angreifer die Dateien anderer Benutzer lesen. Betroffen ist die Version 1.1.2. [http://www.securitytracker.com/alerts/2004/Sep/1011205.html] ■

Courier-IMAP

Ein Format-String-Fehler in Courier-IMAP führt dazu, dass ein entfernter Angreifer Befehle mit den Rechten des Courier-IMAP-Prozesses ausführen kann. Er muss sich nicht authentifizieren. Der Programmierfehler liegt in der Funktion »auth_debug()« (»authlib/debug.c«). Sie führt einen fehlerhaften »fprintf()«-Aufruf aus.

Die Sicherheitslücke ist nur dann ausnutzbar, wenn der Admin in der Konfigurationsdatei den Wert »DEBUG_LOGIN« auf 1 oder 2 eingestellt hat. [http://www.idefense.com/application/poi/display?type=vulnerabilities&id=131] ■

QT-Bibliothek

Die QT-Bibliothek enthält einige Sicherheitslücken. Die Probleme treten auf, wenn die Library bestimmte Bildformate verarbeiten soll. In den Routinen, die für die 8-Bit-RLE-kodierten Formate BMP, XPM, Gif oder Jpeg zuständig sind, treten Heap-Overflows auf. Ein Angreifer kann sie ausnutzen, indem er geschickt manipulierte Bilddateien erzeugt und diese an sein Opfer sendet.

Wenn es die Grafikdateien öffnet, führt das Opfer die Befehle des Angreifers aus. Betroffen ist die Version 3.3.2. [http://www.securitytracker.com/alerts/2004/Aug/1010985.html] ■

CF-Engine

Das »cfservd«-Programm der CF-Engine enthält einen Buffer Overflow in der »AuthenticationDialogue()«-Funktion. Ein entfernter Angreifer kann Befehle mit Root-Rechten ausführen. Er benötigt jedoch eine IP-Adresse, die von der »AllowConnectionsFrom«-Direktive zugelassen ist. Zudem findet sich eine Denial-of-Service-Schwachstelle in »AuthenticationDialogue()«, ein entfernter Angreifer kann die Anwendung zum Absturz bringen.

Betroffen sind die Versionen 2.0.0 bis 2.1.7p1. [http://www.coresecurity.com/common/showdoc.php?idx=387&idxseccion=10] ■

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.

KDE

In KDE wurden mehrere Lücken entdeckt. Läuft eine KDE-Applikation außerhalb der KDE-Umgebung oder unter einer fremden Userkennung, dann prüft sie nicht, ob die Symlinks in »~/.kde« korrekt gesetzt sind. Ein lokaler Angreifer kann dies nutzen und Verzeichnisse manipulieren, auf die diese Symlinks verweisen. Damit kann er Files überschreiben oder dafür sorgen, dass einige KDE-Anwendungen nicht korrekt funktionieren.

Der DCOP-Server legt temporäre Dateien unsicher an. Da DCOP diese Files zur Authentifizierung nutzt, können lokale Angreifer andere Accounts kompromittieren. Ein weiterer Bug tritt auf, wenn ein Benutzer mit KDE Konqueror eine HTML-Seite öffnet, die von einem entfernten Angreifer manipuliert wurde. Konqueror lädt diese Seite eventuell in einem Frame, der zu einer vertrauenswürdigen Webseite gehört. Betroffen sind die Versionen 3.2.3 und älter. [http://www.kde.org/info/security/advisory-20040811-1.txt], [...-2.txt] und [...-3.txt]

Im Konqueror wurde eine weitere Sicherheitslücke gefunden, die so genannte Session-Fixation-Attacken ermöglicht. Um die Websession eines Benutzers zu übernehmen (Session Hijacking), hat ein Angreifer die Wahl zwischen mehreren Techniken: Abhören der SID (Session-ID), Vorhersage der SID oder Erraten per Brute-Force-Attacke. Eine weitere Technik trifft den Konqueror: Der Angreifer weist die SID selbst dem Benutzer zu, noch bevor dieser die Sitzung startet. [http://www.acros.si/papers/session_fixation.pdf]

Im Falle des Konqueror setzen Angreifer ein Cookie für eine Top-Level-Domain. Konqueror sendet dieses Cookie an jeden Webserver in dieser Domain, wenn er die Verbindung öffnet. Im Cookie hat der Angreifer eine von ihm gewählte SID vorgegeben, er kennt diese also und verwendet sie später, um die Sitzung des Opfers zu übernehmen. Betroffen hiervon sind Konqueror 3.2.3 und ältere. [http://www.securitytracker.com/alerts/2004/Aug/1011017.html] ■

Sicherheits-Workshop

Am 2. und 3. März 2005 findet in Hamburg der 12. DFN-CERT Sicherheits-Workshop statt, wieder mit Unterstützung des Linux-Magazins. Die Veranstalter suchen praxisrelevante Beiträge aus den Bereichen Computer- und Netzwerksicherheit, PKI und rechtliche Aspekte. Einsendeschluss für die Kurzfassung der Beiträge ist am 25. Oktober 2004. Weitere Informationen enthält der Call for Papers: [http://www.dfn-cert.de/events/ws/2005/cfp.html]

PostgreSQL

Das von Debian mitgelieferte PostgreSQL enthält eine Sicherheitslücke, durch die ein lokaler Angreifer Logdateien einsehen kann (falsche Zugriffsrechte). Die Logfiles enthalten unter Umständen Account-Daten samt Passwörtern, wenn ein Login-Versuch fehlschlug. Betroffen ist Version 7.4.3-3. [http://www.securityfocus.com/bid/11019] ■

Gaim

Die Installationsroutinen für Gaim-Smiley-Themes sind fehlerhaft. Ein entfernter Angreifer kann Befehle mit den Rechten des Gaim-Users ausführen, wenn der Benutzer ein manipuliertes Theme per Drag&Drop installiert. Betroffen davon ist Gaim vor 0.82. [http://www.securitytracker.com/alerts/2004/Aug/1011082.html]

Wegen zahlreicher Buffer Overflows kann ein entfernter Angreifer ebenfalls Befehle mit den Rechten des Gaim-Anwenders ausführen oder Gaim zum Absturz bringen. Betroffen sind die Versionen vor 0.82. [http://www.securitytracker.com/alerts/2004/Aug/1011083.html] ■

Linux-Kernel

Durch Schwachstellen in einigen USB-Treibern erlangen lokale Angreifer Zugriff auf den Kernelspeicher. Ursache sind nicht-initialisierte Daten in einem »copy_to_user()«-Aufruf. Betroffen davon sind Kernelversionen vor 2.4.27. [http://www.securitytracker.com/alerts/2004/Aug/1011078.html]

Integer-Overflows im Kernel-NFS-Daemon führen dazu, dass ein entfernter Angreifer das System zum Absturz bringen kann. Die Programmierfehler liegen in den XDR-Dekodierfunktionen. Betroffen sind die Kernelversionen 2.4 und 2.6. [http://www.securitytracker.com/alerts/2004/Sep/1011138.html] ■

Imagemagick, Imlib

Durch Buffer Overflows in Imagemagick kann ein entfernter Angreifer die Anwendung zum Absturz bringen. Der Fehler tritt beim Verarbeiten von BMP-Dateien auf, wenn diese RLE-kodiert sind (Run Length Encoding). Betroffen ist Imagemagick vor Version 6.0.6-2. Der Bug steckt in der von Imagemagick genutzten Imlib-Bibliothek, Version 1.9.14. Auch Imlib2 1.1.1 und ältere sind anfällig. [http://bugzilla.gnome.org/show_bug.cgi?id=151034] ■

Bsdmainutils

Eine Schwachstelle in der Calendar-Komponente der Bsdmainutils erlaubt es lokalen Angreifern unter Umständen, Einblick in beliebige Files zu erhalten.

Calendar informiert lokale Benutzer über Events, deren Daten jeder User selbst in einem File in seinem Homeverzeichnis ablegt. In vielen Installationen sendet ein Cronjob den Benutzern eine E-Mail, wenn ein neues Ereignis ansteht: »calendar -a« erledigt dies. Dabei läuft das Tool mit Root-Rechten, die es nicht wieder abgibt.

Der Benutzer kann im Calendar-File allerdings Makros definieren und externe Files per »#include«-Anweisung einbinden – die Calendar-Implementierung nutzt den C-Präprozessor »cpp«, um diese Includes auszuführen. Mit etwas Programmierkenntnissen kann sich der Angreifer beliebige Dateien zusenden lassen. Betroffen sind die Versionen vor 6.0.15. [http://www.securityfocus.com/bid/11077] ■

MySQL

Eine Symlink-Schwachstelle in MySQL führt dazu, dass lokale Angreifer höhere Rechte erlangen können. Fehlerhaft ist »mysqlhotcopy«, das Programm erzeugt temporäre Dateien in »/tmp« mit vorhersagbarem Namen. Dabei achtet es nicht darauf, ob bereits eine Datei gleichen Namens existiert. Betroffen sind die Versionen 4.0.20 und älter. [http://www.securitytracker.com/alerts/2004/Aug/1010979.html]

Ein weiteres Sicherheitsproblem wurde in der »mysql_real_connect()«-Funktion gefunden. Sie prüft DNS-Reverse-Antworten nicht auf ihre Länge. Der »sock_adr.sin_addr«-Puffer ist für die Antwort eventuell zu klein und läuft über. Ein entfernter Angreifer, der DNS-Antworten fälscht, kann damit Befehle auf dem System ausführen. Betroffen sind die Versionen 4.0.20 und älter. [http://www.securitytracker.com/alerts/2004/Aug/1011008.html] ■

Oracle

Im Oracle Database Server wurden gleich mehrere Sicherheitslücken gefunden: Buffer Overflows, SQL-Injection-Probleme und Denial-of-Service-Schwachstellen.

Eine Liste der betroffenen Versionen findet sich unter den URLs: [http://www.idefense.com/application/poi/display?type=vulnerabilities&id=135] sowie [...id=136]

Von vielen Schwachstellen dieser Art ist auch der Oracle Application Server betroffen. [http://www.securitytracker.com/alerts/2004/Sep/1011126.html] ■

Tabelle 2: Linux-Advisories vom 15.08. bis 18.09.04

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

ID	Linux	Fehlerhafte Software
14177	SGI	SGI Propack 3
14178	SGI	SGI Propack 2.4
14179	Debian	CGI-Session-Management in Ruby
14181	Suse	Rsync
14190	Suse	Rsync
14194	Debian	Rsync
14195	Mandrake	Rsync
14196	Debian	KDE-Libs
14209	Mandrake	QT-Bibliothek
14210	Red Hat	Emacs-Erweiterung Semi/Flim
14211	Red Hat	Linux-Kernel
14212	Mandrake	Spamassassin
14213	Red Hat	Netscape 4.8
14214	Red Hat	Pam_wheel und Pam_lastlog
14215	Debian	Mysqlhotcopy
14216	Suse	QT-Bibliothek
14217	Red Hat	Linux-Itanium-Kernel
14243	Mandrake	KDE
14244	Red Hat	QT-Bibliothek
14248	Debian	Icecast-Server
14265	Generisch	Xv
14270	Red Hat	Adobe Acrobat Reader
14271	Mandrake	Linux-Kernel
14272	Generisch	Entrust-Bibliothek Libkmp
14286	SGI	Linux-Kernel des Altix Propack 3
14296	Debian	Python
14297	Debian	QT-Bibliothek
14304	Generisch	ASN.1-Decoder von Kerberos 5
14309	Generisch	MIT Kerberos 5
14312	Mandrake	MIT Kerberos
14313	Debian	MIT Kerberos
14314	Red Hat	MIT Kerberos
14315	Red Hat	MIT Kerberos
14318	Suse	Linux-Kernel
14322	Red Hat	Lha
14324	Red Hat	Mod_ssl
14326	Red Hat	Rsync
14332	Suse	Zlib-Bibliothek
14343	Suse	Mod_ssl-Input-Filter
14348	Red Hat	Gaim
14349	Mandrake	Zlib
14351	Red Hat	Mod_ssl
14353	Mandrake	Cdrecord
14354	Generisch	QT-Bibliothek
14356	Mandrake	Imlib/Imlib2
14357	Red Hat	Lha
14401	Mandrake	Samba 3.0.x
14410	Debian	Webmin
14414	Mandrake	Cups
14415	Mandrake	Foomatic-Filter
14416	Debian	Cups
14417	Red Hat	Cups
14419	Mandrake	Apache 2
14420	Red Hat	Imlib
14421	Red Hat	Midnight Commander (mc)
14422	Mandrake	GDK-pixbuf
14423	Mandrake	Libxpm
14424	Red Hat	Apache 2
14425	Debian	GDK-pixbuf
14426	Mandrake	Libxpm 4
14427	Red Hat	Open Office
14429	Debian	Imagemagick
14430	Mandrake	NTLM-Authentifikation in Squid
14431	Suse	Apache 2
14433	Debian	Imlib
14441	Debian	GTK 2
14442	Suse	GTK 2 und GDK-pixbuf

In Zusammenarbeit mit dem DFN-CERT

Squid

Ein entfernter Angreifer kann eine Denial-of-Service-Attacke gegen Squid durchführen, da der Proxy NTLM-Authentication-Strings nicht korrekt verarbeitet. Um dies auszunutzen, muss ein Angreifer einige ungültige NTLMSSP-Pakete an Squid senden. Er kann den Proxy damit abstürzen lassen.

Der Programmierfehler liegt in der »ntlmGetString()«- und in der »ntlm_fetch_string()«-Funktion. Betroffen ist die Squid-Version 2.5. [http://www.securitytracker.com/alerts/2004/Sep/1011148.html]

Durch eine Buffer-Overflow-Schwachstelle kann ein entfernter Angreifer den Proxy auch zum Absturz bringen. Der Programmierfehler liegt in der »clientAbortBody()«-Funktion. Betroffen sind Version 2.5.STABLE6 und ältere. [http://www.securitytracker.com/alerts/2004/Sep/1011214.html] ■

Acrobat Reader

Ein entfernter Angreifer kann den Adobe Acrobat Reader dazu bringen, beliebige Befehle auszuführen. Er bettet die Kommandos in einen Dateinamen ein und sendet das File UU-kodiert an sein Opfer. Ein weiterer Fehler führt dazu, dass UU-kodierte Dateinamen einen Buffer Overflow hervorrufen. Der Reader prüft die Länge des Dateinamens nicht, bevor er ihn in einen statischen Puffer kopiert. Betroffen sind die Versionen 5.05 und 5.06. [http://www.idefense.com/application/poi/display?type=vulnerabilities&id=124] und [...id=125] ■

Kurzmeldungen

Spamassassin vor 2.64: Fehler beim Verarbeiten von Mailheadern, entfernter Angreifer kann Denial-of-Service-Attacke durchführen. [http://www.securityfocus.com/bid/10957]

Shorewall vor 1.4.10f, 2.0.3a: Symlink-Schwachstelle beim Anlegen von temporären Dateien, lokaler Angreifer kann Files überschreiben. [http://www.securitytracker.com/alerts/2004/Aug/1010915.html]

Quixplorer 2.3 (und älter): Double-Dot-Fehler beim Verarbeiten der »item«-Variablen, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/10949]

Ruby vor 1.6.7 und vor 1.8.1: CGI-Session-Management erzeugt temporäre Dateien mit unsicheren Rechten, lokaler Angreifer kann fremde Sessions übernehmen. [http://www.securityfocus.com/bid/10946]

Gallery 1.4.4: Eingabekontrollfehler in »save_photos.php«-Skript, entfernter, angemeldeter Angreifer mit Upload-Rechten kann Befehle mit Webserver-Rechten ausführen. [http://www.securitytracker.com/alerts/2004/Aug/1010971.html]

J-Shop: Eingabekontrollfehler in »page.php«-Skript, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/11003]

Ulog-php vor 0.8.2: Eingabekontrollfehler in »proto«-Variable, SQL-Injection-Attacke möglich. [http://www.securityfocus.com/bid/11018]

E-Groupware 1.0.0.003: Mehrere Eingabekontrollfehler, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/11013]

Hafiye Sniffer 1.0: Filtert abgehörte Netzwerkdaten nicht, bevor es sie anzeigt, entfernter Angreifer kann Befehle mit Terminal-Escape-Sequenzen einschleusen. [http://www.securitytracker.com/alerts/2004/Aug/1011035.html]

Icecast 1.3.12 und älter (eventuell auch 2.0.x): Eingabekontrollfehler in »list.cgi«, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/11021]

Web-APP: Double-Dot-Fehler in »index.cgi«-Skript, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.securitytracker.com/alerts/2004/Aug/1011053.html]

Hastymail vor 1.0.2: Fehler beim Verarbeiten von Mailanhängen, entfernter Angreifer kann Befehle ausführen. [http://www.securityfocus.com/bid/11022]

PHP Code Snippet Bibliothek: Eingabekontrollfehler in »cat_select«- und »show«-Variablen, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/11038]

IBM DB2 7 und 8: Legt DMS-Verzeichnisse global schreibbar an, lokaler Angreifer kann Dateien manipulieren. Zudem: Buffer Overflow, entfernter Angreifer kann Befehle ausführen. [http://www.securitytracker.com/alerts/2004/Aug/1011060.html] und [.../Sep/1011140.html]

Symantec Gateway Security 1.0, 2.0: Fehler in »isakmpd«, entfernter Angreifer kann Denial-of-Service-Attacke durchführen. [http://www.securitytracker.com/alerts/2004/Aug/1011061.html]

Oracle Enterprise Manager 10g (10.1.0.2): Mehrere unspezifizierte lokale Schwachstellen, die Folgen sind unbekannt. [http://www.securitytracker.com/alerts/2004/Aug/1011110.html]

PHP-Website 0.9.3-4 (und älter): Mehrere Eingabekontrollfehler, Cross-Site-Skripting und SQL-Injection möglich. [http://www.securityfocus.com/bid/11088]

Mailworks Professional: Authentifizierungsfehler im Cookie-Mechanismus, entfernter Angreifer kann administrativen Zugriff erlangen. [http://www.securitytracker.com/alerts/2004/Sep/1011145.html]

Cute News 1.3.6 (und älter): Datei-Include-Fehler durch »cutepath«-Variable, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.7a69ezine.org/node/view/130]

OpenCA vor 0.9.1-9: Eingabekontrollfehler, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/11113]

Neue Releases

Alph: Analysiert und implementiert zahlreiche historische und traditionelle Verschlüsselungsroutinen mit praktischem Pipe-Interface. [http://sourceforge.net/projects/alph/]

BASE (Basic Analysis and Security Engine): Sie analysiert und visualisiert Daten des Snort-IDS. [http://sourceforge.net/projects/secureideas/]

Stegdetect: Entdeckt automatisch steganographischen Inhalt in Dateien. [http://www.outguess.org/download.php]

Rootkit Hunter: Durchsucht das System nach bekannten Rootkits. [http://www.rootkit.nl]

OpenSSH

Ein Eingabekontrollfehler im »scp«-Programm von OpenSSH führt dazu, dass ein entfernter Angreifer Dateien des Client-Systems mit den Rechten des »scp«-Anwenders überschreiben kann.

Zur Attacke benötigt der Angreifer Kontrolle über einen SSH-Server, an dem sich der Client anmelden muss. Betroffen sind die OpenSSH-Versionen vor 3.4p1. [http://www.securitytracker.com/alerts/2004/Sep/1011193.html] ■

MIT Kerberos

Durch fehlerhaftes Speichermanagement im Kerberos-5-KDC (Key Distribution Center) kann ein entfernter Angreifer Befehle einschleusen und damit die komplette Kerberos-Umgebung kompromittieren. Die Sicherheitslücken stecken in den ASN.1-Decoder-Routinen.

Ein weiterer Bug befindet sich in der »krb5_rd_cred()«-Funktion. Sie gibt Speicher frei, der bereits freigegeben ist. Betroffen sind Version 1.3.4 und ältere. [http://www.securitytracker.com/alerts/2004/Aug/1011106.html]

Eine weitere Schwachstelle in der ASN.1-Decoder-Bibliothek führt dazu, dass ein entfernter Angreifer das KDC in einer Endlosschleife festsetzen kann. Der Fehler tritt in der »asn1buf_skiptail()«-Funktion auf, wenn sie auf einen ASN.1-»SEQUENCE«-Typ mit ungültiger Längenangabe trifft. Betroffen sind die Versionen 1.2.2 bis 1.3.4. [http://www.securitytracker.com/alerts/2004/Aug/1011107.html] ■

PHP-Nuke

Durch Eingabekontrollfehler in vielen PHP-Nuke-Modulen gelingen Cross-Site-Skripting-Angriffe. Betroffen ist Version 7. [http://www.systemsecure.org/public/ss23072004.txt]

Ein Authentifizierungsfehler im »admin.php«-Skript führt dazu, dass ein entfernter Angreifer einen Account mit Administrator-Rechten anlegen kann. Der Bug ist zwar längst bekannt und behoben; ein Angreifer kann das Patch aber umgehen, indem er eine »POST«-Anweisung sendet. Betroffen davon ist Version 7.4. [http://www.securitytracker.com/alerts/2004/Sep/1011161.html]

(M. Vogelsberger/fjl) ■

Kurzmeldungen

Serverview 3.0 (eventuell andere): Die ».index«-Datei ist global beschreibbar, lokaler Angreifer kann SNMP-MIB-Werte verändern. [http://www.securityfocus.com/bid/11114]

Star 1.5a09 bis 1.5a45: Falls »star« Set-UID-Root installiert ist und SSH nutzt, kann ein lokaler Angreifer Root-Rechte erlangen. [http://www.securitytracker.com/alerts/2004/Sep/1011195.html]

Apache Mod_ssl 2.0.50: Buffer Overflow in »char_buffer_read()«-Funktion im Reverse-Proxy-Betrieb, entfernter Angreifer kann Apache-Server zum Absturz bringen. [http://www.securitytracker.com/alerts/2004/Sep/1011213.html]

Yapig 0.92b: Eingabekontrollfehler, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securitytracker.com/alerts/2004/Aug/1010970.html]

Xine 0.99.2: Buffer Overflow in Xine-Lib beim Abspielen von Playlists, entfernter Angreifer kann Befehle mit den Rechten des Xine-Anwenders ausführen. [http://www.open-security.org/advisories/6]

Rsync 2.6.2 und älter: Schwachstelle im Daemon-Modus von »rsync«, entfernter Angreifer kann Dateien mit den Rechten des Rsync-Daemon manipulieren. [http://www.securityfocus.com/bid/10938]

Cacti 0.8.5a. Eingabekontrollfehler bei den Benutzernamen- und Passwort-Feldern, daher sind SQL-Injection-Attacken möglich. [http://www.securityfocus.com/bid/10960]

Sara: Mehrere Buffer-Overflow-Schwachstellen in »sarad«, entfernter Angreifer kann Befehle mit den Rechten des Sara-Daemon ausführen. [http://www.securityfocus.com/bid/10984]

Music Daemon 0.0.3: Keine Authentifizierung, entfernter Angreifer kann per »LOAD«- und »SHOWLIST«-Kommando Dateien mit den Rechten des Daemon lesen. [http://www.securityfocus.com/bid/11006]

NSS-Bibliothek: Buffer Overflow beim Verarbeiten von SSLv2-Begrüßungsnachrichten, entfernter Angreifer kann Befehle einschleusen. [http://xforce.iss.net/xforce/alerts/id/180]

Imwheel 1.0.0pre11: Symlink-Schwachstelle beim Anlegen einer temporären Datei mit vorhersagbarem Namen. [http://www.caughq.org/advisories/CAU-2004-0002.txt]

Mpg123 0.59r (eventuell auch 0.59s): Buffer Overflow, entfernter Angreifer kann Befehle mit den Rechten des »mpg123«-Anwenders ausführen. [http://www.alighieri.org/advisories/advisory-mpg123.txt]

GNU Less 358, 381 und 382: Format-String-Fehler in »filename.c« beim Verarbeiten von Dateinamen, lokaler Angreifer kann Befehle einschleusen. [http://www.securitytracker.com/alerts/2004/Aug/1010988.html]

MyDMS 1.4.2 und älter: Eingabekontrollfehler und Double-Dot-Fehler, entfernter Angreifer kann SQL-Injection durchführen sowie Dateien mit Webserver-Rechte lesen. [http://www.securitytracker.com/alerts/2004/Aug/1011014.html]

Mantis 0.19.0a2: Datei-Include-Fehler und Eingabekontrollfehler, entfernter Angreifer kann eigene Befehle einschleusen sowie Cross-Site-Skripting-Attacken durchführen. [http://www.securitytracker.com/alerts/2004/Aug/1011015.html] und [.../1011051.html]

Usermin 1.070 und 1.080: Webmail-Funktion filtert HTML-Nachrichten nicht korrekt, entfernter Angreifer kann Befehle mit den Rechten des Usermin-Benutzers ausführen. [http://www.lac.co.jp/security/csl/intelligence/SNSadvisory_e/77_e.html]

PHP-Fusion: Backup-Dateien in »fusion_admin/db_backups«-Verzeichnis sind öffentlich zugänglich, entfernter Angreifer erfährt unter anderem Benutzernamen und MD5-Hashes der verwendeten Passwörter. [http://www.securitytracker.com/alerts/2004/Aug/1010983.html]