InSecurity News

Atmail

In der Webmail-Applikation Atmail (vom Hersteller auch @mail genannt) wurden zahlreiche Fehler entdeckt. Durch ein typisches Double-Dot-Problem im Perl-Skript »showmail.pl« kann ein entfernter Angreifer die Mailbox von Atmail-Benutzern einsehen. Das Skript prüft den »Folder«-Parameter nicht korrekt. Übergibt der Angreifer in diesem Parameter einen String mit »../«-Sequenzen, erhält er Zugriff auf die Mailboxen anderer User.

Der Angriff gelingt mit der URL »http://*Zielhost*/showmail.pl?Folder=../../*Opfer*@*Zielhost*/mbox/Inbox«. Dieses Sicherheitsproblem tritt jedoch nur bei einer Flat-File-Installation auf.

Falls Atmail jedoch mit SQL-Datenbankunterstützung installiert ist, kann ein entfernter Angreifer einen weiteren Fehler ausnutzen und SQL-Injection-Attacken durchführen. Es handelt sich dabei um Programmierfehler in den Perl-Skripten »readmail.pl«, »atmail.pl« und »search.pl«. Der entfernte Angreifer muss nur sein Sessions-Cookie passend manipulieren, um Zugriff auf die Mailbox eines anderen Users zu erlangen. Voraussetzung ist, dass das Opfer gerade eingeloggt ist.

Ein weiterer Fehler tritt in »showmail.pl« auf, wenn das Skript HTML-Eingaben verarbeitet. Entfernte Angreifer können so Cross-Skripting-Attacken ausführen: »http://*Zielhost*/showmail.pl?Folder=<script>alert(document.cookie)</script>«. Im Inneren des Skript-Tags steht hier eine harmlose Javascript-Anweisung, die lediglich ein neues Fenster öffnet. An ihrer Stelle kann ein Angreifer jedoch auch schädlichen Code einfügen.

Von diesen Schwachstellen ist Version 3.52 betroffen. [http://www.securitytracker.com/alerts/2003/Dec/1008422.html] ■

CVS

Durch eine Sicherheitslücke im Concurrent Versions System (CVS) kann ein entfernter Angreifer Dateien und Verzeichnisse im Root-Directory des CVS-Servers anlegen. Um den Angriff auszuführen, stellt er eine absichtlich falsch formatierte Modul-Anfrage an das System.

Die Auswirkungen dieses Sicherheitsproblems sind jedoch begrenzt – die Rechtevergabe im Dateisystem verhindert die Manipulationen in den meisten Installationen. Anfällig für diese Schwachstelle sind die Versionen vor 1.11.10. [http://www.securityfocus.com/bid/9178] ■

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.

CGI-News und CGI-Forum

Durch mehrere Sicherheitslücken in der CGI-News-Anwendung kann ein entfernter Angreifer die Logdateien einsehen. Ein lokaler Angreifer kann zudem fremde Passwörter erfahren. CGI-News speichert die Passwörter in »*.pwl«-Dateien, die der lokale Angreifer lesen kann. Die Files sind zwar kodiert, der Algorithmus lässt sich aber sehr leicht knacken.
Ein Exploit hierzu findet sich unter der Adresse: [http://www.gulftech.org/vuln/cnc.txt]
Die Logdateien speichert das Newssystem in der Standardkonfiguration gemäß dem Schema »*Benutzername*/*Benutzername*.log«. Ein entfernter Angreifer kann diese vertrauliche Datei lesen.
Betroffen von allen beiden Lücken ist die Version 1.07. [http://www.securitytracker.com/alerts/2003/Dec/1008480.html]
Die gleiche Passwort-Problematik tritt auch in dem Programm CGI-Forum 1.09 auf. [http://www.securitytracker.com/alerts/2003/Dec/1008481.html] ■

Websphere, Coldfusion und J-Run

Aufgrund einer Schwachstelle in IBM Websphere kann ein entfernter Angreifer die Server-CPU für eine gewisse Zeit übermäßig belasten und so einen Denial of Service auslösen. Es genügt, eine geschickt formulierte XML-SOAP-Anfrage an Websphere zu schicken, sie muss spezielle XML-Attribute enthalten. Bei dem Versuch, diese Anfrage zu verarbeiten, beansprucht der XML-Parser von Websphere zu viel CPU-Leistung. Die Voll-Auslastung kann zwischen einigen Sekunden bis zu mehreren Minuten dauern.
Anfällig sind die Versionen 5.0.0, 5.0.1, 5.0.2, 5.0.2.1. [http://www.securitytracker.com/alerts/2003/Dec/1008427.html]
Das gleiche Problem betrifft Macromedia Coldfusion MX 6.0 und 6.1. [http://www.securitytracker.com/alerts/2003/Dec/1008429.html]
Macromedia J-Run 4.0 enthält ebenfalls diesen Fehler. [http://www.securitytracker.com/alerts/2003/Dec/1008430.html] ■

Autorank PHP

Ein Fehler in der Bewertungssoftware Autorank PHP führt dazu, dass ein entfernter Angreifer SQL-Injection-Attacken durchführen kann. Das Problem liegt im PHP-Skript »accounts.php«. Dieses Programm-Modul verarbeitet die »user«-, »username«- sowie »password«-Felder nicht ordentlich. In der Folge kann der Angreifer sogar umfassenden Zugriff auf die Anwendung erlangen.
Von dieser Sicherheitslücke ist die Autorank-Version 2.0.4 betroffen. [http://www.securityfocus.com/bid/9251] ■

Quake-Server

Ein Buffer Overflow in dem Quake-Server »mvdsv« erlaubt es einem entfernten Angreifer, Befehle mit den Rechten des Servers auszuführen. Die Sicherheitslücke liegt in dem Programmteil, der die Download-Funktion implementiert. Ein fertiges Exploit steht unter der URL: [http://packetstorm.linuxsecurity.com/0312-exploits/thttpd-sontot.c].

Betroffen von dem Problem sind die Versionen 0.171 und älter. [http://www.securityfocus.com/bid/9218] ■

Tabelle 2: Linux-Advisories vom 15.12.03 bis 15.01.04

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

ID	Linux	Beschreibung
11203	Mandrake	Schwachstelle in Net-SNMP
11205	Suse	Schwachstelle in LFTP
11221	Mandrake	Schwachstelle in LFTP
11223	Debian	Schwachstelle in Bind 8
11224	Red Hat	Schwachstelle in LFTP
11255	Red Hat	Schwachstellen im Apache
11271	Red Hat	Schwachstelle im Apache
11286	Mandrake	Schwachstellen in IRSSI
11291	Mandrake	Schwachstelle in XFree86
11328	Red Hat	Schwachstelle im 2.4er Kern
11335	Red Hat	Schwachstellen im 2.4er Linux-Kernel
11451	Debian	Schwachstelle im Spiel XSok
11476	Mandrake	Update zur Schwachstelle in ProFTPD
11510	Debian	Schwachstelle in LFTP
11518	Debian	Schwachstellen in Ethereal
11520	Generisch	Schwachstelle in CVS
11521	Debian	Schwachstelle in Screen
11522	Red Hat	Schwachstellen im Linux-Kernel
11534	Suse	Schwachstelle im 2.4er Kern
11535	Debian	Schwachstelle in Bind
11537	Debian	Schwachstelle in Libnids
11538	Debian	Schwachstellen in »nd«
11550	Debian	Format-String-Fehler in »mpg321«
11552	Debian	Schwachstelle im Linux-Kernel
11553	Debian	Schwachstelle in Jabber
11556	Debian	Zwei Schwachstellen in Zebra
11557	Debian	Zwei Schwachstellen in »fsp«
11569	Debian	Schwachstelle im Linux-Kernel (Power-PC)
11578	Debian	Schwachstelle in Vbox3
11579	Red Hat	Zwei Schwachstellen in Ethereal
11597	Debian	Zwei Schwachstellen in PHP-Groupware
11602	Mandrake	Schwachstellen im Linux-Kernel
11603	Generisch	Buffer Overflow in INN
11646	Debian	Schwachstelle im Linux-Kernel (Alpha)
11651	Debian	Schwachstelle in Jitterbug
11660	Debian	Schwachstelle in Mod-Auth-Shadow
11661	Red Hat	Schwachstelle in CVS-Server
11668	Debian	Schwachstelle in CVS-Server
11674	Mandrake	Zwei Schwachstellen in Ethereal
11680	Generisch	Schwachstellen in Implementierungen des H.323-Protokolls
11693	Suse	Schwachstelle in Tcpdump/ISAKMP
11694	Red Hat	Schwachstellen in KDE-Pim
11710	Debian	Schwachstelle im Linux-Kernel (IA64)
11713	Mandrake	Schwachstellen in KDE-Pim
11714	Red Hat	Schwachstelle in Tcpdump/ISAKMP
11715	Suse	Schwachstelle im Linux Kernel (AMD64)

In Zusammenarbeit mit dem DFN-CERT

OS-Commerce

Ein Eingabekontrollfehler im Onlineshop-System OS-Commerce führt dazu, dass ein entfernter Angreifer eine SQL-Injection-Attacke durchführen kann. Der Programmierfehler findet sich in der PHP-Datei »create_account_process.php«. Dieses Skript kontrolliert die Eingabe für das »country«-Feld nicht ordentlich. Fehlerhaft ist auch das PHP-Skript »account_edit_process.php«. Betroffen sind Version 2.2-MS1 und eventuell frühere. [http://www.securitytracker.com/alerts/2003/Dec/1008479.html]

Durch einen weiteren Fehler in der OS-Commerce-Applikation kann ein entfernter Angreifer Cross-Site-Skripting-Attacken ausführen. Die Software filtert die »osCsid«-Variable nicht ordentlich.

Von dem zweiten Programmierfehler ist Version 2.2-MS2 betroffen. [http://www.securitytracker.com/alerts/2003/Dec/1008498.html] ■

Sipd

Im SIP-Daemon (Session Initiation Protocol) von SX-Design wurde eine Sicherheitslücke entdeckt, die ein entfernter Angreifer für eine Denial-of-Service-Attacke ausnutzen kann.

Die Schwachstelle liegt in der Datei »tp/tp.c«. Der Angreifer kann dafür sorgen, dass die Funktion »gethostbyname_r()« einen Wert zurückliefert, den das Programm nicht richtig verarbeiten kann. Er muss beispielsweise versuchen, einen nicht vorhandenen Hostnamen aufzulösen. Dies führt dazu, dass der Server abstürzt. Betroffen ist die Version 0.1.2. [http://www.securityfocus.com/bid/9198]

Ein Format-String-Fehler in »sipd« erlaubt es einem entfernten Angreifer, Speicherbereiche zu manipulieren. Der Fehler tritt auf, wenn der Daemon URI-Argumente verarbeitet. Betroffen hiervon ist die Version 0.1.5. [http://www.securityfocus.com/bid/9236] ■

IRSSI

Ein entfernter Angreifer kann den IRC-Client IRSSI zum Absturz bringen. Voraussetzung ist, dass IRSSI auf einem Rechner läuft, der Speicher-Alignment erzwingt (also kein x86-System), oder dass ein Skript oder ein Plugin das »gui print text«-Signal verwendet. Beispiele dafür sind die beiden Skripte »nicklist.pl« und »tab_stop.pl«. Der Programmierfehler liegt in der Funktion »format_sent_to_gui()« (im Sourcefile »src/fe-common/core/formats.c«). Ein entfernter Angreifer kann dies ausnutzen, indem er eine spezielle IRC-Nachricht an den Client sendet. Dazu benötigt er jedoch Kontrolle über einen IRC-Server.

Anfällig hierfür sind die Versionen vor 0.8.9. [http://www.securityfocus.com/bid/9201] ■

Neue Releases

Rootkit-Hunter: Programm zum Aufspüren von installierten Rootkits. [http://www.rootkit.nl]

Zone-Minder: Programm zur Video-Überwachung unter Linux. [http://www.zoneminder.com/]

LFTP

Eine Buffer-Overflow-Sicherheitslücke in dem FTP- und HTTP-Client LFTP führt dazu, dass ein entfernter Angreifer (mit Kontrolle über einen Webserver) Befehle auf dem Clientsystem ausführen kann. Er erhält so die Rechte des LFTP-Benutzers.

Die Programmierfehler liegen in den beiden Funktionen »try_netscape_proxy()« und »try_squid_eplf()« im Sourcefile »HttpDir.cc«. Ein Angreifer kann dies ausnutzen, indem er auf seinem Webserver speziell konstruierte Verzeichnisse anlegt. Ruft der LFTP-Benutzer auf diesem Server dann »ls« oder einen ähnlichen Befehl auf, kommt es zum Buffer Overflow.

Betroffen davon sind Versionen vor 2.6.10. [http://www.securitytracker.com/alerts/2003/Dec/1008463.html] ■

Visitorbook LE

In der Gästebuch-Software Visitorbook LE wurden zahlreiche Schwachstellen entdeckt. Ein entfernter Angreifer kann über das Gästebuch anonyme E-Mails versenden, falls die »$mailuser«-Variable auf »1« gesetzt ist. Weiterhin kann er dafür sorgen, dass Visitorbook die Logdatei löscht und die Datenbank beschädigt. Das erreicht er, indem er in einem Gästebucheintrag mehr Zeilenumbrüche verwendet, als der Wert in »$max_posts« vorgibt.

Durch einen Eingabekontrollfehler in »visitorbook.pl« beim Verarbeiten der »do«-Variablen kann ein entfernter Angreifer auch Cross-Site-Skripting-Attacken durchführen. Welche Versionen betroffen sind, ist nicht bekannt. [http://www.securitytracker.com/alerts/2003/Dec/1008444.html ■

Mambo-Server

Eine Schwachstelle im Webbasierten Content-Managementsystem Mambo-Server führt dazu, dass ein entfernter Angreifer Konfigurationsvariablen und Benutzerinformationen verändern kann. Ein Programmierfehler in der PHP-Datei »regglobals.php« macht dies möglich. Die Lücke ist jedoch nicht direkt nutzbar, der Angreifer muss den Umweg über ein anderes Skript gehen: »banners.php«, »pollBooth.php«, »upload.php«, »usermenu.php« oder »userpage.php« kommen dafür in Frage.

Einige Beispielexploits finden sich unter der angegebenen Adresse. Betroffen davon sind die Versionen 4.0.14 sowie 4.5 Beta 1.0.3. [http://www.securitytracker.com/alerts/2003/Dec/1008438.html]

Eine weitere Schwachstelle im Mambo-Server erlaubt es einem Angreifer, SQL-Injection-Attacken durchzuführen. Der Programmierfehler liegt in der »show()«-Funktion in »mambo/articles.php«. Er tritt beim Verarbeiten der »$artid«-Variablen auf. Durch diese Attacke gelingt es dem Angreifer eventuell auch, Administrator-Rechte auf dem System zu erlangen.

Betroffen hiervon ist die Version 4.0.14. [http://www.securitytracker.com/alerts/2003/Dec/1008442.html] ■

Ethereal

Im Netzwerk-Sniffer Ethereal wurden zwei Schwachstellen entdeckt. Ein Problem betrifft den Programmteil, der das SMB-Protokoll analysiert. Ein entfernter Angreifer kann es ausnutzen, indem er speziell konstruierte SMB-Daten über das abgehörte Netzwerk schickt. Das zweite Problem steckt im Q.931-Analyseteil des Programms. Mit Hilfe beider Schwachstellen gelingt es einem entfernten Angreifer, Ethereal zum Absturz zu bringen.

Betroffen von dieser Lücke sind die Versionen vor 0.10.0. [http://www.securityfocus.com/bid/9248] und [.../9249] ■

Dada-Mail

In der Mailinglisten-Software Dada-Mail wurden zwei Sicherheitsprobleme gefunden. Zunächst sind die von Dada generierten PIN-Nummern für einen Angreifer vorhersagbar und damit unsicher. In der Folge kann der Angreifer unwissende Benutzer auf die Mailingliste setzen. Außerdem kann sich ein entfernter Angreifer mit einem beliebigen Passwort in eine Liste einloggen, falls kein Listenpasswort gesetzt ist.

Betroffen von diesem Problem ist die Version 2.8.10. [http://www.securitytracker.com/alerts/2003/Dec/1008521.html] ■

Indent

Ein Heap-Overflow-Fehler im Indent-Programm erlaubt es entfernten und lokalen Angreifern, Befehle in das System einzuschleusen. Die Kommandos laufen mit den Rechten des Indent-Anwenders. Der Overflow tritt in der Funktion »handle_token_colon()« auf. Ein Angreifer kann dies ausnutzen, indem er eine C-Datei geschickt konstruiert. Wendet sein Opfer Indent auf die manipulierte Datei an, führt es die Befehle des Angreifers aus.

Anfällig für dieses Problem ist Version 2.2.9. [http://www.securityfocus.com/bid/9297] ■

Apache Mod_php

Aufgrund einer Sicherheitslücke in der Kombination aus Apache 2 und dem Modul Mod_php kann ein lokaler Angreifer unter Umständen die HTTPS-Verbindungen anderer Benutzer übernehmen. Apache und Mod_php geben viele Dateideskriptoren an den PHP-Interpreter weiter. Dazu gehört auch der Deskriptor, der für die HTTPS-Verbindung zuständig ist. Der Angriff kann unter Umständen sogar von einem entfernten Angreifer durchgeführt werden – er muss dazu jedoch eigene PHP-Skripte auf den Webserver kopieren und dort ausführen dürfen.

Betroffen von diesem Problem sind PHP 4.2 und 4.3 mit Apache 2.0. [http://www.securityfocus.com/bid/9302] ■

Kurzmeldungen

Mini-BB 1.7 (und älter): Eingabekontrollfehler im »bb_edit_prf.php«-Skript, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9310]

BNC-Web: Fehler in »BNCquery.pl«, entfernter Angreifer kann Files mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/9181]

XOOPS 2.0.5.1: Fehler im PHP-Skript »myheader.php« beim Verarbeiten der »$url«-Variablen, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9269]

Sara 4.2.6, 4.2.7 (eventuell andere): Eingabekontrollfehler beim Auswerten von Protokoll-Bannern, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2003/Dec/1008499.html]

ECW-Shop 5.01, 5.5: Fehler beim Filtern des »cat«-Parameters, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9244]

Project-Forum und **Course-Forum** 8.4.2.1 (und älter): Fehler beim Verarbeiten von »find«-Strings und Eingabekontrollfehler bei HTML-Eingaben, entfernter Angreifer kann die Anwendung zum Absturz bringen; Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2003/Dec/1008537.html] und [[.../1008538.html]]

L-Soft Listserv: Fehler bei URL-Verarbeitung, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9307]

GKrellm 2.1.19: Legt Passwörter unverschlüsselt im lokalen Dateisystem ab, lokale Angreifer können Mail-Passwörter anderer Benutzer lesen. [http://www.securitytracker.com/alerts/2003/Dec/1008564.html]

PHP-Nuke Surveys-Modul 7.0 Final: Fehler beim Verarbeiten der Variablen »pollID«, SQL-Injection-Attacke möglich. [http://www.securityfocus.com/bid/9305]

PHP-Ping: Fehler beim Prüfen der »$count«-Variablen in »php-ping.php«, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/9309]

CVS-Pserver 1.11.10 (und älter): Fehler tritt auf, wenn ein lokaler Angreifer Schreibzugriff auf »$CVSROOT/CVSROOT/passwd« hat, er kann dann Befehle mit Root-Rechten ausführen. [http://www.securitytracker.com/alerts/2003/Dec/1008568.html]

PHP-Catalog 2.6.7 (und älter): Fehler beim Filtern der »id«-Variablen, SQL-Injection möglich. [http://www.securityfocus.com/bid/9318]

VCard4J: Fehler beim Einlesen von V-Cards, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Jan/1008582.html]

Easy-Dynamic-Pages 2.0: Datei-Include-Fehler in »admin/config.php« und »dynamicpages/fast/config_page.php«, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securitytracker.com/alerts/2004/Jan/1008584.html]

LDU-Forum 601: Eingabekontrollfehler in »auth.php«, SQL-Injection-Attacken möglich (sogar ohne sich anzumelden). [http://www.securitytracker.com/alerts/2003/Dec/1008416.html]

W-Agora-Forum vor 4.1.6: Eingabekontrollfehler in »include/auth.php3«, »editform.php3«, »modules.php3«, »index.php3«, »insert.php3«, »update.php3« und »browse.php3«, Datei-Include-Exploits und Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2003/Dec/1008483.html]

Bes-cms vor 0.5rc4: Datei-Include-Fehler, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securitytracker.com/alerts/2003/Dec/1008536.html]

Surfboard-Webserver 1.1.9: Buffer Overflow bei »GET«-Anfragen mit mehr als 1024 Zeichen, entfernter Angreifer kann Befehle mit Server-Rechten ausführen. [http://www.securityfocus.com/bid/9299]

P-Serv 3.0 beta2: Double-Dot-Schwachstelle, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/9276]

Knowledge-Builder: Include-Fehler in »index.php« beim Verarbeiten der »page«-Variablen, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/9292]

Subscribe Me Pro Enterprise

Aufgrund einer Sicherheitslücke in der Mailinglisten-Software Subscribe Me kann ein entfernter Angreifer Befehle mit Webserver-Rechten ausführen. Der Programmierfehler liegt im »setup.pl«-Skript. Ein Beispiel-Exploit findet sich unter der Webadresse: [http://www.pimp-industries.com/pimp-0003.txt]
Das Advisory enthält keine Informationen dazu, welche Versionen betroffen sind. [http://www.securitytracker.com/alerts/2003/Dec/1008524.html] ■

Open BB und PHP BB

Ein entfernter Angreifer kann wegen eines Programmierfehlers in der Open-BB-Anwendung SQL-Injection-Attacken gegen die zugrunde liegende Datenbank ausführen. Das Problem liegt im »index.php«-Skript, es verarbeitet den »CID«-Parameter nicht korrekt. Der Angreifer kann damit an die Hashes von Passwörtern gelangen und versuchen, diese mit Brute-Force-Attacken zu knacken. Betroffen ist die Version 1.0.6. [http://www.securitytracker.com/alerts/2003/Dec/1008555.html] ■

Ein ähnliches Problem betrifft auch PHP BB. SQL-Injection-Attacken erfordern hier jedoch Moderator-Rechte seitens des Angreifers. Der Programmierfehler liegt in »groupcp.php«. Das Skript nutzt die »$sql_in«-Variable ungeprüft, um mit ihr eine SQL-Datenbankabfrage zu konstruieren. Ein entfernter Angreifer kann diese Variable geschickt setzen und damit beliebige SQL-Anweisungen einschleusen. [http://www.securitytracker.com/alerts/2003/Dec/1008571.html] ■

Squirrelmail

Ein Eingabekontrollfehler in Squirrelmail führt dazu, dass ein entfernter Angreifer Befehle mit Webserver-Rechten ausführen kann. Das Skript »gpg_encrypt.php« prüft die Variable »send_to_bcc« nicht ordnungsgemäß. Ein Angreifer nutzt dies, indem er eine Mail mit speziell konstruiertem »To:«-Feld verwendet. Der Angriff gelingt nur, wenn das Opfer das GPG-Verschlüsselungs-Plugin verwenden. [http://www.securitytracker.com/alerts/2003/Dec/1008548.html] ■

Unix-2-TCP

Ein Buffer-Overflow-Fehler wurde in Unix-2-TCP gefunden (das Tool leitet Unix-Sockets auf TCP-Verbindungen weiter). Ein lokaler Angreifer kann höhere Rechte erlangen. Der Overflow tritt auf, wenn »unix2tcp« bestimmte Kommandozeilenparameter verarbeitet. Voraussetzung ist, dass das Programm mit Set-UID-Rechten installiert ist.
Betroffen von dem Problem sind die Versionen vor 0.8.0. [http://www.securityfocus.com/bid/9240] *(M. Vogelsberger/fjl)* ■