InSecurity News

NFS-Utils

Eine Schwachstelle in den NFS-Utils führt dazu, dass ein entfernter Angreifer den »rpc.mountd«-Dienst zum Absturz bringen kann. Der Fehler in der »get_reliable_hostbyaddr()«-Funktion (in der Datei »support/export/hostname.c«) tritt auf, wenn ein Client einen ungültigen DNS-Eintrag besitzt.

Der Angreifer muss auf einen Reverse-DNS-Lookup mit einer speziell konstruierten Antwort reagieren, braucht also Zugriff auf den DNS-Server für seinen IP-Bereich. Betroffen sind die Versionen vor 1.0.6. [http://www.securityfocus.com/bid/9813] ■

Tcpdump

In Tcpdump wurden zwei Schwachstellen entdeckt. In »print-isakmp.c« tritt ein Buffer Overflow auf, wenn der Sniffer ISAKMP-Delete-Pakete mit einer zu hohen Zahl von SPIs (Security Protocol Identifier) verarbeiten muss. Tcpdump stürzt ab – vorausgesetzt es wurde mit der Option »-v« aufgerufen.

Wenn Tcpdump ISAKMP-Identification-Pakete mit einer Payload-Länge von weniger als 8 empfängt, stürzt der Sniffer ebenfalls ab.

Betroffen davon sind die Versionen vor 3.8.2. [http://www.securitytracker.com/alerts/2004/Mar/1009593.html] ■

Interscan Viruswall und Clam Antivirus

In Trend Micros Interscan Viruswall führt eine Double-Dot-Schwachstelle dazu, dass ein entfernter Angreifer Dateien mit den Rechten des integrierten Proxy-Servers lesen kann. Er muss in einer URL nur ausreichend viele »../«-Zeichen einfügen, um beliebige Dateien zu lesen. Betroffen davon ist die Version 3.5. [http://www.securityfocus.com/bid/9966]

Ein Angreifer kann Clam Antivirus zum Absturz bringen. Der Programmierfehler in »unrarlib« tritt auf, wenn Clam bestimmte RAR-Dateien verarbeitet. Die stammen unter anderem vom Bagle-Wurm. Betroffen sind die Versionen vor 0.68. [http://www.securitytracker.com/alerts/2004/Mar/1009502.html]

Durch eine Schwachstelle in Clams Virus-Event-Direktive kann ein lokaler Angreifer Befehle mit Root-Rechten ausführen. Er erzeugt eine Datei, deren Name einen Virus-String und Shell-Befehle enthält. Bemerkt Clam diese Datei, ruft der Scanner die »virusaction()«-Funktion auf. Diese leitet den Dateinamen an einen »system()«-Aufruf weiter, ohne auf Shell-Sonderzeichen zu achten. [http://www.securitytracker.com/alerts/2004/Apr/1009615.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/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.	

Apache-Module

In mehreren Apache-Modulen finden sich Sicherheitslücken. Ein Problem in Mod_ssl führt dazu, dass ein entfernter Angreifer den Server zum Absturz bringen kann. Um die Lücke in der Funktion »ssl_io_filter_disable()« (in »ssl_engine_io.c«) auszunutzen, sendet der Angreifer Klartext-HTTP-Anfragen an den SSL-Port des Webservers. Betroffen sind die Versionen 2.0.35 bis 2.0.48. [http://www.securitytracker.com/alerts/2004/Mar/1009337.html]

Ein Fehler in Mod_access führt dazu, dass Apache einige »allow«- und »deny«-Regeln auf Big-Endian-Plattformen mit 64-Bit-Architektur missachtet. Der Server übersieht Regeln, die IP-Adressen ohne Netzmaske enthalten. Angreifer erlangen Zugriff, auch wenn der Webmaster ihre IP-Adresse gesperrt hat. Betroffen sind die Versionen 1.3.29 und älter. [http://www.securitytracker.com/alerts/2004/Mar/1009338.html]

Das Mod_disk_cache-Modul enthält ebenfalls Fehler, es speichert Account-Informationen auf der Festplatte des Webservers. Darunter sind auch Passwörter als Klartext. Betroffen sind die Versionen 2.0.49 und älter. [http://www.securitytracker.com/alerts/2004/Mar/1009509.html]

Ein Off-By-One-Overflow im Mod-Security-Modul erlaubt es einem entfernten Angreifer, Befehle mit den Webserver-Rechten auszuführen. Die Schwachstelle lässt sich nur ausnutzen, wenn die Option »SecFilterScanPost« aktiviert ist. Eine geschickt formulierte HTTP-»POST«-Anfragen ruft den Overflow hervor. Betroffen ist die Version 1.7.4 für den Apache 2.x. [http://www.securitytracker.com/alerts/2004/Mar/1009445.html]

Ein Eingabekontrollfehler im Mod_survey-Modul führt dazu, dass ein entfernter Angreifer Cross-Site-Skripting-Attacken ausführen kann. Die betroffenen Versionen finden sich unter der angegebenen Adresse. [http://www.securitytracker.com/alerts/2004/Mar/1009516.html] ■

PHP-BB

In PHP-BB wurden gleich mehrere Schwachstellen entdeckt. Über die »viewforum«- und »viewtopic«-Skripte sind Cross-Site-Skripting-Attacken ausführbar. Beide Programme filtern die »topicdays«-Variable nicht ordentlich. Ein entfernter Angreifer schleust damit Javascript-Befehle in den Sicherheitskontext der PHP-BB-Seite ein und erlangt Zugriff auf Authentifizierungsdaten des Opfers. Betroffen davon sind die Versionen 2.0.6d und älter. [http://www.securitytracker.com/alerts/2004/Mar/1009421.html]

Durch einen Eingabekontrollfehler in »search.php« gelingen einem entfernten Angreifer SQL-Injections. Die Attacke ist nur möglich, wenn »register_global« aktiviert ist. Die Applikation formuliert intern eine SQL-Abfrage, in die sie benutzerdefinierte Eingaben aus der »show_results«-Variablen einbettet. Mit geschickt formulierten Daten schleust der Angreifer eigene SQL-Anweisungen ein. Betroffen sind die Versionen 2.0.6 und älter. [http://www.securitytracker.com/alerts/2004/Mar/1009423.html]

Weitere SQL-Injection-Fehler finden sich in »admin_smilies.php« und »admin_styles.php«. Auch Cross-Site-Skripting ist möglich. Das Problem tritt beim Verarbeiten der Parameter »id« oder »style_id« auf. Betroffen sind Version 2.0.7a und ältere. [http://www.securitytracker.com/alerts/2004/Mar/1009510.html]

Eingabekontrollfehler in dem »profile.php«-Skript von PHP-BB 2.0.6d erlauben ebenfalls Cross-Site-Skripting-Attacken aus der Ferne. [http://www.securitytracker.com/alerts/2004/Mar/1009519.html]

Fehler beim Verarbeiten der »pm_sql_user«-Variable in »privmsg.php« führen zu einer weiteren Schwäche für SQL-Injection-Attacken. Betroffen ist die Version 2.0.8. [http://www.securitytracker.com/alerts/2004/Mar/1009563.html] ■

Neue Releases

Rootkit Hunter: Das Programm spürt Rootkits auf. [http://www.rootkit.nl]

Web Application Worms – Myth or Reality: Das Paper erklärt, auf welche Weise sich Würmer über Webdienste verbreiten. [http://www.imperva.com/application_defense_center/white_papers/default.asp]

Tabelle 2: Linux-Advisories vom 15.03. bis 15.04.04

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

ID	Linux	Beschreibung
12582	Debian	Schwachstelle in Samba
12602	Debian	Schwachstelle in GDK-Pixbuf
12615	Generisch	Denial-of-Service-Schwachstellen in OpenSSL
12616	Suse	Denial-of-Service-Schwachstellen in OpenSSL
12617	Red Hat	Denial-of-Service-Schwachstellen in OpenSSL
12618	Red Hat	Denial-of-Service-Schwachstellen in OpenSSL
12631	Mandrake	Denial-of-Service-Schwachstellen in OpenSSL
12632	Debian	Denial-of-Service-Schwachstellen in OpenSSL
12634	Red Hat	Denial-of-Service-Schwachstellen in OpenSSL
12638	Red Hat	Schwachstellen in Mozilla
12640	Debian	Schwachstelle im Linux-Kernel 2.2 für PowerPC
12701	Red Hat	Speicherleck in Apache-2-Modul Mod_ssl
12720	Generisch	Zwei Schwachstellen in Ecartis
12721	Debian	Schwachstellen in Emil
12740	SCO	Überarbeitete Pakete beheben Schwachstelle in »mc«
12742	Debian	Buffer Overflow in Mutt
12766	Red Hat	Schwachstelle in Squid
12776	Debian	Fehlende Eingabeprüfung/SQL-Injektion bei PAM-Pgsql
12784	Red Hat	Schwachstellen in Mozilla
12792	Red Hat	Schwachstellen in Ethereal
12793	Mandrake	Schwachstellen in Ethereal
12794	Red Hat	Schwachstellen in Ethereal
12795	Mandrake	Schwachstelle in Squid
12808	SCO	Schwachstelle in Vim
12809	SCO	Schwachstelle in Util-Linux
12811	Debian	Schwachstelle im Perl-Modul Safe.pm
12848	Debian	Buffer Overflow im Editor Vfte
12849	Debian	Schwachstelle in Oftpd
12850	Debian	Schwachstellen in Squid
12853	Debian	Update: Race Condition in Sysstat
12856	Debian	Schwachstelle in Interchange
12858	Debian	Schwachstellen im HPPA-Linux-Kernel 2.4.18
12865	Mandrake	Schwachstelle in Mplayer
12876	Debian	Race Condition in Xine-ui
12877	Debian	Zwei Schwachstellen in Tcpdump
12880	Debian	Cross-Realm-Schwachstelle in Heimdal
12936	Mandrake	Schwachstelle in IPsec/IKE
12951	Mandrake	Schwachstellen in Tcpdump
12953	Red Hat	Schwachstelle in Cadaver-Bibliothek Neon
12954	Red Hat	Schwachstellen in Cadaver-Bibliothek Neon
12956	Mandrake	Schwachstellen im Linux-Kernel
12957	Suse	Schwachstellen im Linux-Kernel
12961	Suse	Schwachstelle in CVS
12962	Suse	Schwachstelle in CVS
12963	Red Hat	Schwachstelle in CVS
12964	Red Hat	Schwachstelle in CVS
12965	Mandrake	Schwachstelle in CVS
12966	Debian	Schwachstellen im Linux-Kernel (Alpha)
12967	Debian	Schwachstellen im Linux-Kernel (HPPA)
12968	Debian	Schwachstellen im Linux-Kernel (IA64)
12969	Debian	Schwachstellen im Linux-Kernel (Apus, S390)
12970	Red Hat	Schwachstelle in Open-Office-Bibliothek Neon
12971	Debian	Schwachstellen im Linux-Kernel (i386)

In Zusammenarbeit mit dem DFN-CERT

Konqueror und Opera

Der KDE Konqueror verarbeitet Cookies fehlerhaft. Ein entfernter Angreifer kann Zugriff auf fremde Cookies erlangen. Diese enthalten eventuell auch sicherheitsrelevante Informationen, zum Beispiel die Session-IDs einer anderen Sitzung. [http://www.securitytracker.com/alerts/2004/Mar/1009363.html]

Das gleiche Problem betrifft den Opera-Browser in Versionen vor 7.21. [http://www.securitytracker.com/alerts/2004/Mar/1009365.html]

Opera begeht zudem Fehler beim Verarbeiten von übergroßen Arrays in Javascript-Code. Ein entfernter Angreifer kann den Browser zum Absturz bringen, indem er passenden Skript-Code in eine HTML-Seite einbindet und sein Opfer dazu bringt, die Seite aufzurufen. Betroffen von der Denial-of-Service-Schwachstelle ist Opera 7.23. Eventuell lässt sich auch Code einschleusen. [http://www.securityfocus.com/bid/9869] ■

PHP-Nuke und Addons

Mehrere Eingabekontrollfehler in PHP-Nuke führen zu Schwächen für Cross-Site-Skripting. Die Fehler sind in vielen Programmteilen zu finden (siehe URL). Betroffen ist die Version 7.1.0. [http://www.securitytracker.com/alerts/2004/Mar/1009439.html]

Im 4n-Album-Modul wurden mehrere Sicherheitslecks gefunden: eine Datei-Include-Schwachstelle in »display-category.php« (nur ausnutzbar, wenn »allow_url_fopen« gesetzt ist), Cross-Site-Skripting in »nmimage.php« beim Verarbeiten der »z«-Variablen und SQL-Injection (die »gid«-Variable wird nicht korrekt überprüft). Betroffen ist die Version 0.92. [http://www.securitytracker.com/alerts/2004/Mar/1009449.html]

Auch das 4n-Guestbook-Modul enthält Bugs. Ein Eingabekontrollfehler beim Handling der »entry«-Variablen führt zu Cross-Site-Skripting. Ein Bug in »admin.php« gestattet SQL-Injection-Attacken. Das Skript filtert die »nbid«-Variable nicht richtig. Betroffen ist die Version 0.92. [http://www.securitytracker.com/alerts/2004/Mar/1009450.html] ■

WU-Ftpd

Durch eine Sicherheitslücke in WU-Ftpd kann ein entfernter, angemeldeter Angreifer den Zugangsschutz umgehen. Der Angreifer ändert die Rechte seines Homeverzeichnisses so, dass er selbst nicht mehr darauf zugreifen darf. Meldet er sich erneut am FTP-Server an, erhält er sofort Zugriff auf das FTP-Verzeichnis. Betroffen ist die Version 2.6.2 [http://www.securityfocus.com/bid/9832] ■

Courier

Wegen einiger Buffer-Overflow-Fehler im Mailserver Courier kann ein entfernter Angreife Befehle mit den Rechten des Servers ausführen. Die Overflows treten beim Verarbeiten von Unicode-Zeichen in »iso2022jp.c« und »shiftjis.c« auf. Ein Angreifer kann dies ausnutzen, indem er einen manipulierten Unicode-Text an sein Opfer schickt. Dieser Text muss Zeichen außerhalb des Bereichs der Basic Multilingual Plane enthalten.

Betroffen von den Overflows sind die Versionen vor 3.0.0. [http://www.securitytracker.com/alerts/2004/Mar/1009455.html] ■

Python

Ein Buffer Overflow in der »getaddrinfo()«-Funktion von Python führt dazu, dass ein Angreifer unter Umständen Befehle mit höheren Rechten ausführen kann. Er muss eine geschickt konstruierte IPv6-Adresse per DNS verbreiten. Wenn in Python die IPv6-Unterstützung deaktiviert ist, berücksichtigt der Programmcode nicht, dass eine DNS-Auflösung eine IPv6-Adresse zurückliefern könnte. Diese Adressen sind jedoch länger als IPv4-Adressen und führen daher zum Überlauf.

Betroffen sind die Versionen 2.2 und 2.2.1. [http://www.securityfocus.com/bid/9836] ■

Lotus Domino

Im Lotus Domino Webserver wurde ein Double-Dot-Fehler gefunden. Ein entfernter, angemeldeter Administrator kann so Dateien außerhalb des Webverzeichnisses anlegen. Der Programmierfehler tritt in der »webadmin.nsf/dlgFilesFolderNew«-Funktion auf. Ein Angreifer kann auch testen, ob eine Datei auf dem System schon vorhanden ist. Ein weiterer Eingabekontrollfehler in der Funktion »Quick Console« führt zu Cross-Site-Skripting.

Betroffen von beiden Lücken ist Version 6.5.1. [http://www.securitytracker.com/alerts/2004/Mar/1009446.html] ■

OpenSSL

In OpenSSL wurden mehrere Schwachstellen gefunden. Ein Fehler steckt in der Funktion »do_change_cipher_spec()«. Ein entfernter Angreifer kann mit ihr im SSL/TLS-Handshake die OpenSSL-Anwendung abstürzen lassen. Betroffen sind die Versionen 0.9.6c bis 0.9.6k und 0.9.7a bis 0.9.7c.

Ein weiteres Problem tritt bei SSL/TLS-Handshakes mit Kerberos auf. Ein entfernter Angreifer kann ebenfalls die Anwendung zum Absturz bringen. Anfällige Versionen sind 0.9.7a, 0.9.7b, 0.9.7c. [http://www.securitytracker.com/alerts/2004/Mar/1009458.html] ■

Ethereal

Durch Sicherheitslücken in Ethereal kann ein entfernter Angreifer Befehle auf dem System ausführen. Die Fehler treten beim Verarbeiten einiger Protokolle auf: Netflow, IGAP, EIGRP, PGM, IRDA, BGP, ISUP und TCAP. Ein Angreifer muss manipulierte Pakete über das überwachte Netzwerk senden.

Betroffen sind die Versionen 0.8.13 bis 0.10.2. [http://www.securityfocus.com/bid/9952] ■

SOAP-Nachrichten

Einige Anwendungen haben Probleme, SOAP-Nachrichten korrekt zu verarbeiten. Einem entfernten Angreifer gelingen daher Denial-of-Service-Angriffe. Anfällig sind Sun Java Application Server 7.0 bis Update 2 [http://www.securitytracker.com/alerts/2004/Mar/1009429.html] sowie der Macromedia JRun Server 4.0 [.../1009430.html] und Macromedia Coldfusion Server 6.0 und 6.1 [.../1009431.html]. ■

Sysstat

In Sysstat wurden einige Probleme gefunden. Die »post«- und »trigger«-Skripte sowie das »isag«-Programm sind anfällig für eine Symlink-Schwachstelle. Sie erzeugen ohne weitere Sicherheitsvorkehrungen temporäre Dateien in »/tmp«. Unter Umständen kann ein lokaler Angreifer höhere Rechte erlangen. [http://www.securitytracker.com/alerts/2004/Mar/1009377.html] sowie [.../1009378.html] ■

Kurzmeldungen

Myproxy: Eingabekontrollfehler bei URL-Verarbeitung, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9846]

V-Host vor 3.10r1: Fehlerhafte Eingabekontrolle bei HTML-Verarbeitung, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9860]

Xitalk 1.1.11: Lokaler Angreifer kann Befehle mit UTMP-Gruppenrechten ausführen. [http://www.securityfocus.com/bid/9851]

Oracle Application Server 9.0.4.0.0, 9.0.3.1.0, 9.0.2.3.0 und 9.0.0.4.0: Oracle nennt weder Ursache noch Folgen dieser Sicherheitslücke. [http://www.securitytracker.com/alerts/2004/Mar/1009419.html]

YaBB 1 Gold (SP1.3), 1.5.1: Eingabekontrollfehler in »[glow]«- und »[shadow]«-Tags, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Mar/1009428.html] und [.../1009427.html]

Phorum 5.0.3 Beta (und älter): Eingabekontrollfehler in »register.php«, »login.php« und »profile.php«, Cross-Site-Skripting ist möglich. [http://www.securityfocus.com/bid/9882]

PAM-Pgsql 0.5.2-5: Eingabekontrollfehler in den Funktionen »auth_verify_password()« und »pam_sm_chauthtok()«, SQL-Injection-Attacke möglich. [http://www.securitytracker.com/alerts/2004/Mar/1009584.html]

V-Bulletin 3.0.0 RC4 (und älter): Eingabekontrollfehler in den PHP-Skripten »showthread.php«, »forumdisplay.php« und »memberlist.php«, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Mar/1009440.html]

Pegasi 0.2.2: Double-Dot-Fehler und Fehler bei der Eingabekontrolle, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen und Cross-Site-Skripting ausführen. [http://www.securitytracker.com/alerts/2004/Mar/1009396.html]

PHP-X 2.0 bis 3.2.4: Schwachstelle beim Erzeugen der Session-IDs, entfernter Angreifer kann Verbindungen anderer Benutzer übernehmen (Session Hijacking). [http://www.securityfocus.com/bid/9569]

Blogger: Eingabekontrollfehler im Benutzerprofil, Cross-Site-Skripting-Angriffe möglich. [http://www.securitytracker.com/alerts/2004/Mar/1009560.html]

Tarantella Enterprise 3.40, 3.3x und 3.2x: Eingabekontrollfehler in »ttaarchives.cgi« und »ttacab.cgi«, Cross-Site-Skripting-Angriffe möglich. [http://www.securitytracker.com/alerts/2004/Mar/1009501.html]

PHP 4.1.2 (und älter, 4.x): Speichert Session-IDs im »/tmp«-Verzeichnis, lokale Angreifer können damit die Webverbindungen übernehmen. [http://www.securitytracker.com/alerts/2004/Mar/1009525.html]

PHP 3.0 bis 4.1.0: Fehler im Sicherheitsmodus »safe_mode«, entfernter Angreifer kann Schutzmechanismen umgehen. [http://www.securitytracker.com/alerts/2004/Mar/1009536.html]

Nstxd 1.1-beta3 (und älter): Fehler beim Tunneln über den UDP-Port 53, entfernter Angreifer kann Server zum Absturz bringen. [http://www.securitytracker.com/alerts/2004/Mar/1009567.html]

PS-Include vor 1.42: Mangelhafte Filterung der »template«-Variablen, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/10006]

Nessus 2.0.10a (eventuell andere): Legt Account-Daten als Klartext in ».nessusrc« ab, lokaler Angreifer kann diese lesen. [http://www.securitytracker.com/alerts/2004/Mar/1009575.html]

Sillysearch vor 2.4: Eingabekontrollfehler beim Verarbeiten von URLs, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Mar/1009598.html]

Mozilla Mail 1.4 und älter: Probleme beim Verarbeiten von SMIME-Mails mit speziellen ASN.1-Daten, entfernter Angreifer kann so Befehle mit den Rechten des Mozilla-Anwenders ausführen. [http://www.securitytracker.com/alerts/2004/Mar/1009479.html]

PHPKIT 1.6.03 (eventuell andere): Einige Eingabekontrollfehler, Cross-Site-Skripting und SQL-Injection möglich. [http://www.securitytracker.com/alerts/2004/Mar/1009599.html]

Squidguard

Wegen eines Bugs in Squidguard kann ein entfernter Angreifer die Zugangskontrollen umgehen. In die Adresse bettet er ein URL-kodiertes Null-Byte ein: »http://blablabla%00*@www.verbotene-seite.de*« gibt ihm Zugang zu der verbotenen Site. [http://www.securityfocus.com/bid/9919] ■

M-Player

Durch einen Heap Overflow in M-Player kann ein entfernter Angreifer mit Kontrolle über einen Server Befehle in den Client einschleusen. Betroffen sind die Versionen 1.0pre3 und älter. [http://www.securityfocus.com/bid/10008] ■

C-Panel

In C-Panel kann ein entfernter Angreifer beliebige Befehle mit Root-Rechten ausführen. Das Skript für das Zurücksetzen des Passworts lässt Shell-Sonderzeichen in einem Eingabefeld zu. Betroffen sind Version 9.1.0 Build 34 und ältere. [http://www.securitytracker.com/alerts/2004/Mar/1009400.html]

Entfernten Angreifern ist wegen eines Bugs in »dohtaccess.html« auch Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Mar/1009402.html]

Ähnliche Bugs finden sich in »dodelautores.html« und »addhandle.html« in Version 9.1.0-STABLE 93. [http://www.securitytracker.com/alerts/2004/Mar/1009541.html] ■

Isakmpd

Der ursprünglich aus OpenBSD stammende »isakmpd« ist für Authentifizierung und Schlüsselaustausch in IPsec zuständig. Sicherheitslücken beim Verarbeiten der Nutzdaten führen dazu, dass ein entfernter Angreifer den Daemon zum Absturz bringen kann. Die Programmierfehler in »doi.h«, »util.h«, »ipsec.c«, »isakmp_doi.c« und »message.c« bringen das Speichermanagement durcheinander. [http://www.securitytracker.com/alerts/2004/Mar/1009468.html] ■

GDK-Pixbuf

Ein Bug in der GDK-Pixbuf-Bibliothek führt dazu, dass ein entfernter Angreifer Anwendungen, die GDK-Pixbuf nutzen, abschießen kann. Zum Beispiel stürzt Evolution bei einer geschickt konstruierten Bitmap-Datei ab. Betroffen sind die Versionen vor 0.20. [http://www.securityfocus.com/bid/9842] ■

MySQL

Eine Symlink-Schwachstelle in der MySQL-Komponente »mysqlbug« erlaubt es lokalen Angreifern, Dateien mit Root-Rechten zu überschreiben. Mysqlbug achtet beim Anlegen der temporären Datei »/tmp/failed-mysql-bugreport« nicht darauf, ob diese schon existiert.

Betroffen davon sind die Versionen 4.0.18 und älter. [http://www.securityfocus.com/bid/9976] *(M. Vogelsberger/fjl)* ■

Kurzmeldungen

Open Webmail 2.30 und älter: Eingabekontrollfehler in »userstat.pl«, entfernter Angreifer kann eigene Befehle einschleusen. [http://www.securitytracker.com/alerts/2004/Mar/1009406.html]

Mad BMS 1.1.4 (und älter): Fehler im Anmeldevorgang, entfernter Angreifer kann unberechtigt Zugriff auf das System erlangen. [http://www.securityfocus.com/bid/10018]

Imgsvr 0.4: Fehler bei URL-Verarbeitung, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.securitytracker.com/alerts/2004/Apr/1009620.html]

Mambo Open Source 4.5 Stable 1.0.3 und älter: Eingabekontrollfehler, SQL-Injection und Cross-Site-Skripting sind möglich. [http://www.securitytracker.com/alerts/2004/Mar/1009447.html]

X-Web 1.0: Double-Dot-Fehler, entfernter Angreifer kann Daten mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/9937]

P-Webserver 0.3.3: Double-Dot-Fehler, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/9817]

Mathopd-Webserver 1.4p2 und 1.5b13: Buffer Overflow in »prepare_reply()« (in »request.c«), entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/9871]

Borland Interbase 7.1: Die »admin.ib«-Datei ist global beschreibbar, lokale Angreifer können Benutzeraccounts hinzufügen und sich die Administratorrechte für die Datenbank verschaffen. [http://www.securityfocus.com/bid/9929]

Xine: Symlink-Schwachstelle beim Anlegen von »/tmp/xine-bugreport«, lokaler Angreifer kann Daten mit den Rechten des Xine-Anwenders manipulieren. [http://www.securityfocus.com/bid/9939]

SSH Tectia Server 4.0.3 und 4.0.4: Fehler bei den Routinen zum Ändern von Passwörtern, entfernter Angreifer erfährt den privaten Host-Key des Servers. [http://www.ssh.com/company/newsroom/article/520/]

Linux-Kernel »kmod« 2.4: Kmod setzt seine Rechte nicht richtig, lokaler Angreifer kann durch Signale an Kmod einen Absturz bewirken. [http://www.securitytracker.com/alerts/2004/Mar/1009534.html]

Ridentd 0.9.1b: Symlink-Schwachstelle in »rident.pl« (speichert eine PID in »/tmp/rident.pid«), lokaler Angreifer kann Dateien mit Root-Rechten überschreiben. [http://www.securitytracker.com/alerts/2004/Mar/1009552.html]

Oftpd 0.3.6: Der »PORT«-Befehl verarbeitet nur Portnummern bis 255, ein entfernter Angreifer kann den Server zum Absturz bringen. [http://www.securityfocus.com/bid/9980]

OpenLDAP-Backend »back-ldbm« vor 2.1.17: Schwachstelle in »slapd/back-ldbm/passwd.c«, entfernter Angreifer kann den LDAP-Server zum Absturz bringen. [http://www.securitytracker.com/alerts/2004/Apr/1009627.html]

Fizmez Webserver 1.0: Stürzt ab, wenn der Client über eine HTTP-Verbindung keinerlei Daten sendet. [http://www.autistici.org/fdonato/advisory/fws1.0-adv.txt]

Automake vor 1.8.3: Symlink-Schwachstelle in »/lib/am/distdir.am«, lokaler Angreifer kann Files mit den Rechten des Automake-Anwenders überschreiben. [http://www.securityfocus.com/bid/9816]

GTK-See 0.5.1 und älter: Heap-Overflow beim Verarbeiten von PNG-Bildern, entfernter Angreifer kann die Rechte des GTK-See-Anwenders erlangen. [http://www.securityfocus.com/bid/8061]

Emil 2.1.0-beta9 und älter: Buffer-Overflow- und Format-String-Fehler beim Verarbeiten von Mime- und UU-kodierten Mails, entfernter Angreifer kann Befehle auf dem System ausführen. [http://www.securityfocus.com/bid/9974]

Samba-Beispielskript »smbprint«: Symlink-Schwachstelle beim Erzeugen von »/tmp/smb-print.log«, lokaler Angreifer kann Dateien mit den Rechten des Smbprint-Anwenders überschreiben (in neueren Versionen muss dazu in ».config« das Debugging aktiviert sein). [http://www.securityfocus.com/bid/9926]