InSecurity News

Apache

In dem Apache-Modul Mod_cplusplus wurde ein Buffer Overflow gefunden, der Fehler liegt in der Datei »cpp_request.cpp«. Die Folgen sind unbekannt. Betroffen sind die Versionen 1.4 und älter. [http://www.securitytracker.com/alerts/2004/Sep/1011238.html]

Eine Schwachstelle im Modul Mod_dav versetzt einen entfernten Angreifer in die Lage, eine Denial-of-Service-Attacke durchzuführen. Er benötigt dazu das Recht, die »LOCK«-Methode aufzurufen. Betroffen sind Version 2.0.50 und ältere. [.../1011248.html]

Ein Fehler beim Parsen einer IPv6-Adresse führt dazu, dass entfernten Angreifern eine Denial-of-Service-Attacke gelingen kann. Sie sorgen dafür, dass »memcpy()« eine negative Längenangabe erhält, um einen Segmentation Fault in »apr-util/test/testuri.c« und »apr-util/uri/apr_uri.c« auszulösen. Betroffen hiervon sind die Versionen vor 2.0.51. [.../1011299.html]

Eine weitere Denial-of-Service-Attacke ist möglich, wenn Apache SSL-Verbindungen verarbeitet. Der Angreifer kann einen Kindprozess in eine Endlosschleife bringen. Betroffen hiervon sind die Versionen vor 2.0.51. [.../1011340.html]

Durch ein Problem beim Verarbeiten von Konfigurations- und ACL-Dateien kann ein lokaler Angreifer Befehle mit Webserver-Rechten ausführen. Für die Attacke erzeugt er eine spezielle ».htaccess«- oder »httpd.conf«-Datei, die einen Buffer Overflow in der Funktion »ap_resolve_env()« auslöst (»server/util.c«). Betroffen sind die Versionen vor 2.0.51. [.../1011303.html]

Durch einen Fehler beim Handling der »Satisfy«-Direktive kann ein entfernter Angreifer Zugriff auf für ihn gesperrte Ressourcen erlangen. Betroffen ist die Version 2.0.51. [.../1011385.html] ■

Realplayer

In Realplayer wurden zahlreiche Schwachstellen gefunden. Ein entfernter Angreifer kann Befehle mit den Rechten des Realplayer-Anwenders ausführen, wenn der User eine manipulierte RM-Datei abspielt. Ein entfernter Angreifer kann auch eine spezielle Website konstruieren, die beim Besuch beliebige Befehle auf dem Anwendersystem ausführt.

Durch weitere Schwachstellen kann ein entfernter Angreifer Dateien löschen. Betroffen hiervon sind die Versionen vor 10.5 (6.0.12.1016). [http://www.securitytracker.com/alerts/2004/Sep/1011449.html] ■

Tabelle 1: Sicherheit bei den großen Distributionen

Distributor	Quellen zur Sicherheit	Bemerkungen
Debian	Infos: [http://www.debian.org/security/] Liste: [http://lists.debian.org/debian-security-announce/] Betreff: DSA-... [1]	Bei Debian sind die aktuellen Security Advisories bereits auf der Homepage zu finden. Die Meldungen sind als HTML-Seiten mit Links zu den Patches realisiert. Die Sicherheitsseite enthält auch Hinweise zur Mailingliste.
Gentoo	Infos: [http://www.gentoo.org/security/] Liste: [http://www.gentoo.org/main/en/lists.xml] (gentoo-announce und gentoo-security) Betreff: GLSA: ... [1]	Auf der Gentoo-Website ist seit dem Frühjahr 2004 ein eigener Bereich zu Sicherheitsaktualisierungen und anderen Security-Informationen zu finden. Die Sicherheitsseite ist vorbildlich auf der Homepage verlinkt. Die Advisories liegen als HTML-Seiten vor.
Mandrake	Infos: [http://www.mandrakesecure.net] Liste: [http://www.mandrakesecure.net/en/mlist.php] (announce) Betreff: MDKSA-... [1]	Mandrakesoft betreibt eine eigene Website zu Sicherheitsthemen. Sie enthält unter anderem Security Advisories und Hinweise zu den Mailinglisten. Die Advisories sind zwar HTML-Seiten, die Patches darin aber nicht verlinkt.
Red Hat	Infos: [http://www.redhat.com/security/] Liste: [http://www.redhat.com/mailman/listinfo/] (Enterprise-watch-list und Redhat-watch-list) Betreff: [RHSA-... [1]	Red Hat listet Security Advisories unter »Support I Security and Updates« für jede unterstützte Version, derzeit vor allem für die Enterprise-Ausgaben. Die Security Advisories liegen als HTML-Seite vor, die Patches sind darin aber nicht verlinkt.
Slackware	Infos: [http://www.slackware.com/security/] Liste: [http://www.slackware.com/lists/] (slackware-security) Betreff: [slackware-security] ... [1]	Die Startseite verlinkt direkt zum Archiv der Security-Mailingliste. Darüber hinaus sind auf der Homepage jedoch keine Informationen zur Sicherheit von Slackware zu finden.
Suse	Infos: [http://www.suse.de/security/] Patches: [http://www.suse.de/de/support/download/updates/] Liste: suse-security-announce Betreff: [suse-security-announce] ... [1]	Die Sicherheitsseite ist nach einer Änderung der Homepage nicht mehr direkt verlinkt. Sie enthält Infos zur Mailingliste sowie die Advisories. Die Sicherheitspatches zu den einzelnen Suse-Linux-Versionen sind in der allgemeinen Updates-Seite rot markiert und mit einer kurzen Beschreibung der geschlossenen Lücke versehen.

[1] Alle Distributoren kennzeichnen ihre Security-Mails im Betreff.

Xinelib

Mehrere Stack-Overflow-Sicherheitslücken in Xinelib erlauben es einem entfernten Angreifer, Befehle mit den Rechten des Xine-Anwenders auszuführen. Die Overflows treten beim Einlesen von Video-CD-MRLs mit überlangen Strings auf (Media Resource Locator). Ein Angreifer benutzt für seine Aktionen eine entsprechend manipulierte »vcd://«-MRL.

Weitere Probleme treten beim Handling von nicht terminierten ISO-Disk-Labels sowie bei bestimmten Untertiteln auf. Betroffen sind die Xinelib-Versionen 1-rc2 bis 1-rc5. [http://www.securitytracker.com/alerts/2004/Sep/1011336.html]

Ein Heap Overflow beim Verarbeiten von DVD-Subpictures führt ebenfalls dazu, dass ein entfernter Angreifer Befehle mit den Rechten des Xine-Users ausführen kann. Betroffen hiervon sind die Xinelib-Versionen 1-rc2 bis 1-rc5 sowie ältere Ausgaben. [.../1011337.html] ■

BEA Weblogic Server und Express

Einige interne, an den JNDI-Baum gebundene Serverobjekte von BEA Weblogic Server und Express sind nicht korrekt geschützt, ein entfernter Angreifer kann auf sie zugreifen. Betroffen sind die Versionen 6.1 SP6, 7.0 SP5 und 8.1 SP2 (und älter). [http://www.securitytracker.com/alerts/2004/Sep/1011226.html]

Ein entfernter Angreifer mit RMI-Zugriff kann durch einen Bug im Administrationsserver unberechtigt »weblogic.Admin«-Befehle ausführen. Betroffen sind BEA 7.0 SP5 und 8.1 SP2 (und älter). [.../1011227.html]

Wenn Weblogic unter Linux läuft und Anwendungen von einem Filesystemen lädt, das die Groß- und Kleinschreibung von Dateinamen ignoriert, passen einige URL-Muster in »web.xml« nicht. Ein entfernter Angreifer kann dadurch Zugriffskontrollen umgehen. Betroffen sind 6.1 SP6, 7.0 SP5 und 8.1 SP2 (und älter). [.../1011228.html]

Einige Skripte enthalten Passwörter im Klartext. Ein lokaler Angreifer kann sie lesen. Betroffen sind BEA 6.1 SP6, 7.0 SP4 und 8.1 SP2 (und älter). [.../1011229.html]

Nach dem Booten des Systems muss der Admin ein Passwort eintippen, das in manchen Fällen bei der Eingabe als Klartext angezeigt wird. Betroffen sind BEA 6.1 SP6, 7.0 SP5 und 8.1 SP2 (und älter). [.../1011230.html]

Wenn beim Einrichten der Security-Roles und -Policies ein interner Fehler in einem Security Provider auftritt, laufen Anwendungen mit unvollständigen Sicherheitsregeln. Betroffen sind BEA 7.0 SP5 und 8.1 SP2 (und älter). [.../1011232.html]

Auf BEA-Systeme, die zur User-Authentifizierung einen Active-Directory-LDAP-Server nutzen, kann ein entfernter Angreifer trotz gesperrtem Account zugreifen. Betroffen sind 7.0 SP5 und 8.1 SP2 (und älter). [.../1011233.html]

Falls der Admin-Port nicht aktiviert ist, kann ein Angreifer im lokalen Netzwerk sicherheitsrelevante Daten abhören. Dazu gehört auch das Admin-Passwort. Auch kann er Konfigurationsdaten während der Übertragung manipulieren. Betroffen sind die Weblogic-Versionen 7.0 und 8.1. [.../1011234.html] ■

Webmin, Usermin

Das »maketmp.pl«-Skript von Webmin und Usermin enthält eine Schwachstelle, die einem lokalen Angreifer unter Umständen Root-Rechte gibt. Das Skript achtet beim Anlegen des Temp-Verzeichnisses »/tmp/.usermin« nicht darauf, ob es schon existiert. Betroffen sind die Usermin-Versionen vor 1.089. [http://www.securitytracker.com/alerts/2004/Sep/1011267.html] und Webmin vor 1.159. [.../1011268.html] ■

Session-Fixation-Angriffe bei vielen Webbrowsern

Bei der recht neuen Crackertechnik Session Fixation manipulieren die Angreifer Cookies. Sie setzen ein neues Cookie im Browser des Benutzers, noch bevor dieser auf eine Website geht, die das gleiche Cookie setzen und abfragen würde. Der Angreifer kennt das von ihm vorgegebene Cookie und kann daher die üblichen Authentifizierungs-Mechanismen, die auf Session-IDs mit Cookies basieren, umgehen.

Per Default sendet der Browser ein Cookie an alle Ports, über reines HTTP oder per SSL. Das »secure«-Attribut bestimmt, dass ein Cookie nur über einen sicheren SSL-Kanal verschickt werden darf. Das soll verhindern, dass sensitive Informationen (etwa Session-IDs) über unsichere Kanäle laufen. Es gibt jedoch keinen Mechanismus, der verhindert, dass ein auf unsicherem Weg gesetztes Cookie auch über SSL versendet wird. Ein Angreifer kann also selbst dann Session-Fixation-Attacken durchführen, wenn die Website das Secure-Flag setzt.

Auch das »domain«-Attribut bereitet Schwierigkeiten. Es legt fest, an welche Domains das Cookie noch gesendet werden darf. Top-Level-Domains wie ».de« werden von den Browsern automatisch verboten, Einträge mit nur einem Punkt erlauben sie nicht. Viele Browser akzeptieren jedoch Einträge, die eine große Domain freigeben. Wendet der Angreifer diesen Trick zusammen mit einer Session-Fixation-Attacke an, kann er noch größeren Schaden anrichten.

Viele Browser sind von diesen Problemen betroffen. Der Autor des Advisories hat Internet Explorer 6.0, Konqueror 3.1.4, Mozilla Firefox 0.9.2 und Opera 7.51 getestet. Info: [http://www.westpoint.ltd.uk/advisories/wp-04-0001.txt] ■

Tabelle 2: Linux-Advisories vom 19.09. bis 15.10.04 (In Zusammenarbeit mit dem DFN-CERT)

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

ID	Linux	Fehlerhafte Software	ID	Linux	Fehlerhafte Software
14452	Generisch	Mozilla, Firefox und Thunderbird	14600	Suse	Samba
			14601	Debian	Mod_dav in Apache 2
14453	Suse	Libxpm	14602	Suse	Mozilla
14456	Mandrake	Gdk-Pixbuf	14603	Red Hat	XFree86
14460	Debian	Wv	14604	Debian	Net-Acct
14468	Debian	Lukemftpd	14609	Debian	Samba
14477	Debian	Imlib2	14610	Mandrake	Xinelib
14478	Red Hat	Redhat-config-nfs	14621	Debian	Libxpm
14479	Red Hat	Samba	14622	Mandrake	Cyrus-SASL/Libsasl
14480	Mandrake	Mpg123	14623	Red Hat	Cyrus-SASL/Libsasl
14481	Mandrake	Webmin	14639	Debian	MySQL
14482	Mandrake	Imagemagick	14640	Debian	Python
14516	Debian	Getmail	14641	Debian	Libxpm in XFree86
14526	Debian	Sendmail	14644	Red Hat	Flim
14527	Mandrake	Open Office	14647	Red Hat	Ethereal
14531	Mandrake	NetPBM	14648	Red Hat	Rsync
14558	Debian	Freenet6	14659	Red Hat	Squirrelmail
14560	Red Hat	Mozilla	14660	Debian	Cyrus-SASL
14561	Red Hat	Squid	14662	Debian	CVS-Server
14562	Red Hat	Ruby	14665	Debian	Cyrus-SASL
14564	Red Hat	Tcpdump	14668	SCO	PNG-Bibliothek
14565	Red Hat	Spamassassin	14669	SCO	Cups
14566	Red Hat	Cadaver	14671	Debian	Mpg123
14579	Mandrake	Samba	14672	Debian	Sox
14580	Red Hat	Cadaver	14673	Debian	Cyrus-SASL
14582	Debian	Netkit-Telnet-Server	14677	Debian	Cups
14584	Debian	Netkit-Telnet-Server	14678	Red Hat	PHP
14585	Debian	PPPOE	14679	Red Hat	NetPBM
14587	Red Hat	Samba	14683	Red Hat	Apache-Webserver und -Module
14594	Red Hat	XFree86	14684	Red Hat	Samba
14595	Red Hat	KDE	14685	Red Hat	Lha

Linux-Kernel

Eine Schwachstelle im Code zum Handling von TCP-Sockets im Linux-Kernel erlaubt es, dass lokale Angreifer eine Denial-of-Service-Attacke gegen das Linux-System ausführen. Der Angriff führt dazu, dass der Kernel einen Socket wieder verwendet, obwohl ihn der ursprüngliche Erzeuger noch nicht geschlossen hat. Damit braucht der Kernel alle verfügbaren Sockets auf. Betroffen ist die Version 2.4.27. [http://www.securitytracker.com/alerts/2004/Sep/1011245.html]

Eine weitere Sicherheitslücke wurde in der SG_IO-Funktionalität (SCSI Generic IO) des IDE-CD-Moduls gefunden. Durch diese Schwachstelle kann ein lokaler Angreifer unberechtigte Schreib- und Lösch-Operationen auf dem betroffenen Medium ausführen. [.../1011412.html] ■

PHP

Ein Fehler in der »phpinfo()«-Funktion von PHP erlaubt es einem entfernten Angreifer, Speicherbereiche des Systems auszulesen. Der Fehler tritt beim Verarbeiten eines Array auf. Betroffen sind »GET«, »POST« und »COOKIES« in PHP 5.0 bis 5.0.1. [http://www.securitytracker.com/alerts/2004/Sep/1011279.html]

Ein weiterer Fehler findet sich im Quellcode »rfc1867.c« in der Funktion »SAPI_POST_HANDLER_FUNC()«. Ein entfernter Angreifer kann Elemente des »$_FILES«-Array überschreiben. Betroffen davon sind PHP 5.0.1 und älter. [.../1011307.html] ■

Mozilla, Thunderbird und Firefox

In Mozilla, Thunderbird und Firefox wurden Sicherheitslücken gefunden. Ein entfernter Angreifer kann dadurch Befehle mit den Rechten des Browsers ausführen oder per Cross-Site-Skripting die Rechte übernehmen, die eine Webseite dem Browser-Benutzer gewährt.

Die Send-Page-Funktion verarbeitet überlange URLs nicht richtig. Durch einen Heap Overflow kann ein entfernter Angreifer Befehle mit den Rechten des Anwenders ausführen. [http://bugzilla.mozilla.org/show_bug.cgi?id=258005]

Per Javascript-Code kann ein entfernter Angreifer auf das Clipboard des Mozilla-Benutzers zugreifen und so eventuell private Inhalte sehen. [.../show_bug.cgi?id=257523]

Ein entfernter Angreifer kann sich mit einem signierten Skript höhere Rechte verschaffen und so den Inhalt von Dialogboxen verändern. [.../show_bug.cgi?id=253942]

Beim Verarbeiten von V-Cards kann ein Buffer Overflow auftreten. Der Fehler liegt im File »addrbook/src/nsVCardObj.cpp«. [.../show_bug.cgi?id=257314]

Eine Schwachstelle für Cross-Site-Skripting wurde ebenfalls entdeckt. [.../show_bug.cgi?id=250862]

Ein Integer Overflow kann auftreten, wenn Mozilla manipulierte BMP-Bilder verarbeitet. Ein entfernter Angreifer kann eine entsprechende Datei an sein Opfer schicken und dann Kommandos mit den Rechten dieses Anwenders ausführen. [http://www.zencomsec.com/advisories/mozilla-1.7.2-BMP.txt]

URLs mit Hostnamen, die Nicht-Ascii-Zeichen enthalten, können einen Heap Overflow auslösen. Ein entfernter Angreifer kann dann möglicherweise Befehle mit Anwenderrechten ausführen. [.../mozilla-1.7.2-UTF8link.txt]

Auch im POP3-Code wurde eine Sicherheitslücke gefunden. Der Buffer-Overflow-Fehler kann eventuell dazu führen, dass ein Angreifer eigene Befehle einschleust. [.../mozilla-1.7.2-POP3.txt] ■

Neue Releases

On Polymorphic Evasion: Der Text beschreibt die Verwendung von polymorphem Shellcode. [http://seclists.org/lists/bugtraq/2004/Oct/0022.html]

Phishing Attacks: Paper, das Wege beschreibt, um an Nutzerdaten zu kommen. [http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf]

Exploits fehlerhafter PHP-Skripte: Das DFN-CERT berichtet, dass Schwachstellen in unsicheren PHP-Skripten derzeit vermehrt ausgenutzt werden. [http://www.linux-community.de/story?storyid=14590]

IBM RSCT

IBM RSCT (Reliable Scalable Cluster Technology) enthält eine Schwachstelle, durch die ein lokaler Angreifer Dateien beschädigen oder neu erzeugen kann.

Über »ctstrtcasd -f *Datei*« legt RSCT ein File mit Root-Rechten an und schreibt 65535 Bytes Trace-Daten hinein. Betroffen sind die Versionen 2.3.0.0 und älter. [http://www.securitytracker.com/alerts/2004/Sep/1011429.html] ■

Kurzmeldungen

Perldesk: Double-Dot-Fehler bei der »lang«-Variable, entfernter Angreifer kann Systemdateien lesen. [http://www.securitytracker.com/alerts/2004/Sep/1011276.html]

Cups: Fehler in »scheduler/dirsvc.c« beim Handling einiger UDP-Pakete auf Port 631, Denial of Service möglich. [http://www.securitytracker.com/alerts/2004/Sep/1011283.html]

Foomatic vor 3.0.2: Schwachstelle in Foomatic-rip, entfernter Angreifer mit Druckrecht kann Befehle mit »lp«-Rechten ausführen. [http://www.securityfocus.com/bid/11184]

Sudo 1.6.8: Fehler in der Sudoedit-Option »-u«, lokaler Angreifer mit Sudoedit-Rechten kann Dateien mit höheren Rechten lesen. [http://www.securityfocus.com/bid/11204]

PHP-Groupware vor 0.9.16.003: Eingabekontrollfehler im Wiki-Modul (»transforms.php«), Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/11130]

Remository: Eingabekontrollfehler, SQL-Injection möglich. [http://www.securitytracker.com/alerts/2004/Sep/1011356.html]

Latex2rtf 1.9.15: Buffer Overflow in »expandmacro()«-Funktion, entfernter Angreifer kann Befehle mit den Rechten des Latex2rtf-Anwenders ausführen. [http://www.securityfocus.com/bid/11233]

Redhat-config-nfs vor 1.0.13-6: Das Programm setzt falsche Rechte für exportierte Shares, entfernter Angreifer kann unberechtigt Zugriff auf Daten erlangen. [http://www.securityfocus.com/bid/11240]

MySQL vor 4.1.5: Buffer Overflow in Libmysqlclient. [http://www.securitytracker.com/alerts/2004/Sep/1011408.html]

Flc 1.0.4 (und älter): Buffer Overflow beim Verarbeiten der Kommandozeilenparameter (»flc.c«), lokaler Angreifer kann Befehle mit den Rechten des »flc«-Prozesses ausführen. [http://www.nosystem.com.ar/advisories/advisory-06.txt]

Fprobe vor 1.0.6: Nicht weiter spezifizierte Lücke im Change-User-Feature. [http://www.securityfocus.com/bid/11255]

Debian Sendmail 8.12.3, 8.13.1: Die »sasl-bin«-Installation setzt einen Standardaccount mit bekanntem Passwort, entfernter Angreifer kann unerlaubt Mails versenden. [http://www.securityfocus.com/bid/11262]

Peoplesoft HRMS 7: Eingabekontrollfehler in Debugging- und Utility-Skripten, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Sep/1011433.html]

Parachat-Server 5.5: Double-Dot-Fehler, entfernter Angreifer kann Dateien des Systems mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/11272]

Icecast 2.0.1 (und älter): Buffer Overflow beim Verarbeiten bestimmter HTTP-Anfragen, entfernter Angreifer kann Befehle mit den Rechten des Icecast-Servers ausführen. [http://www.securityfocus.com/bid/11271]

Serendipity 0.7-beta1 und älter: Mehrere Eingabekontrollfehler, Cross-Site-Skripting und SQL-Injection möglich. [http://www.securityfocus.com/bid/11269]

Debian Freenet6 vor 0.9.6-1: Die Datei »/etc/freenet6/tspc.conf« ist global lesbar, lokaler Angreifer kann das Tunnel-Broker-Passwort lesen. [http://www.securityfocus.com/bid/11280]

Samba 2.2 bis 2.2.11, 3.0 bis 3.0.5: Eingabekontrollfehler beim Verarbeiten von MSDOS-Pfadnamen, entfernter Angreifer kann unberechtigt auf Dateien außerhalb des Share-Pfads zugreifen. [http://www.securityfocus.com/bid/11281]

Rip-MIME vor 1.4.0.0: Schwachstellen beim Verarbeiten von MIME-Inhalten. [http://www.securitytracker.com/alerts/2004/Sep/1011237.html]

SUS 2.0.2: Format-String-Fehler in der »log()«-Funktion, lokaler Angreifer erhält Root-Rechte. [http://www.securityfocus.com/bid/11176]

Macromedia JRun, Coldfusion MX

Im Macromedia JRun-Server wurden zahlreiche Schwachstellen entdeckt. Durch einen Bug beim Umgang mit JSession-IDs hat ein entfernter Angreifer die Chance, Sitzungen anderer User zu übernehmen oder Session Fixation durchzuführen.

Eingabekontrollfehler in der Management-Konsole erlauben es einem entfernten Angreifer, Cross-Site-Skripting- und Session-Fixation-Attacken auszuführen. Ein entfernter Angreifer kann durch ein weiteres Sicherheitsleck den Quelltext von ».cfm«-Dateien sehen. Ist der Verbose-Modus aktiviert, dann tritt in den Logging-Routinen ein Buffer Overflow auf. Betroffen von diesen Sicherheitsproblemen sind die Versionen 3.0, 3.1 und 4.0. [http://www.securitytracker.com/alerts/2004/Sep/1011404.html]

Einige dieser Schwachstellen finden sich auch in Coldfusion MX. [.../Sep/1011405.html] Durch eine weitere Schwachstelle in Coldfusion MX kann ein entfernter, angemeldeter Angreifer das Administrator-Passwort lesen – vorausgesetzt er darf Templates anlegen. Betroffen ist die Version 6.1. [.../Oct/1011475.html] ■

W-Agora

In W-Agora wurden zahlreiche Eingabekontrollfehler gefunden. Die meisten führen zu Cross-Site-Skripting und SQL-Injection. Es ist aber auch eine neue Angriffstechnik aufgetaucht: Response-Splitting-Attacken.

An solchen Angriffen sind drei Parteien beteiligt:

- ein Webserver mit einem speziellen Sicherheitsleck,
- ein Zielobjekt (meist ein HTTP-Proxy-Cache),
- ein Angreifer.

Durch eine Fehlfunktion des Servers kann der Angreifer dafür sorgen, dass er auf eine HTTP-Anfrage zwei HTTP-Antworten erhält. Den Inhalt der zweiten Antwort kann er beliebig vorgeben. Nach einer solchen Anfrage sendet der Angreifer eine zweite, normale Anfrage an den Webserver, der wieder eine Antwort – die dritte – liefert. Das Zielobjekt (etwa ein Proxy) verfolgt den Datenverkehr und glaubt fälschlicherweise, die zweite vom Server geschickte Antwort gehöre zur zweiten HTTP-Anfrage des Angreifers. So ordnet der Proxy-Cache der Ressource aus der normalen Anfrage den vom Angreifer beliebig konstruierten Inhalt zu.

Greifen später andere Anwender über den Proxy-Cache auf diese Ressource zu, erhalten sie die Seite des Angreifers statt des wahren Inhalts. Damit kann ein Angreifer einen Web-Cache vergiften (Web-Cache-Poisoning-Attacke). Weitere Folgen von Response Splitting diskutiert das Whitepaper: [http://www.sanctuminc.com/pdf/whitepaper_httpresponse.pdf]

Von dem Webserver-Problem ist W-Agora 4.1.6a betroffen. [http://www.securitytracker.com/alerts/2004/Sep/1011463.html]

(M. Vogelsberger/fjl) ■

Kurzmeldungen

Online Recruitment Agency und **Real Estate Management** vor 1.1: »site.xml« ist öffentlich zugänglich, entfernter Angreifer kann das SQL-Datenbank-Passwort lesen. [http://securitytracker.com/alerts/2004/Oct/1011539.html] und [.../1011540.html]

Silent Storm Portal 2.1, 2.2: Eingabekontrollfehler, Cross-Site-Skripting möglich; entfernter Angreifer kann Administrator-Rechte erlangen. [http://www.cyberspy.org/gam/silentstorm.multiple]

Roaring Penguin PPPOE-Treiber 3.5 (und älter): Fehler in den Kommandozeilenoptionen »-D« und »-p«, lokaler Angreifer kann fremde Dateien manipulieren. [http://www.securityfocus.com/bid/11315]

Bugport vor 1.134: Fehler beim Verarbeiten von Datei-Attachements. [http://securitytracker.com/alerts/2004/Oct/1011543.html]

Blackboard 1.5.1: Datei-Include-Fehler in »bb_lib/admin.inc.php«, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://securitytracker.com/alerts/2004/Oct/1011551.html]

Cubecart 2.0.1: Eingabekontrollfehler in »index.php«, SQL-Injection möglich. [http://securitytracker.com/alerts/2004/Oct/1011560.html]

IBM DB2 8.1 Fixpak 7 (und älter): Zahlreiche Buffer-Overflow-Fehler, entfernter Angreifer kann unberechtigt Befehle ausführen. [http://securitytracker.com/alerts/2004/Oct/1011562.html]

Helix Universal Server: Fehler beim Verarbeiten bestimmter HTTP-»POST«-Header, entfernter Angreifer kann Denial-of-Service-Attacke ausführen. [http://www.securityfocus.com/bid/11352]

GDK-pixbuf 0.22 und älter: Endlosschleife bei fehlerhaften BMP-Bildern, Heap- und Stack-Overflows bei XPM-Dateien sowie Absturz bei manipulierten ICO-Files. [http://www.securityfocus.com/bid/11195]

Libxpm in X11 R6.8.0: Einige Integer- und Stack-Overflows, entfernter Angreifer kann Befehle mit Anwenderrechten ausführen. [http://scary.beasts.org/security/CESA-2004-003.txt]

Getmail vor 3.2.5 und vor 4.2.0: Symlink-Schwachstelle, lokaler Angreifer kann Dateien mit fremden Rechten manipulieren. [http://www.securityfocus.com/bid/11224]

Tutos 1.1 und älter: Eingabekontrollfehler, SQL-Injection und Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Sep/1011363.html]

Mambo Server: Datei-Include-Fehler in Cache-library (»mosConfig_absolute_path«-Variable) und Cross-Site-Skripting-Lücke in »index.php«. [http://www.securitytracker.com/alerts/2004/Sep/1011365.html]

Jabberd 1.4.3 (und älter) sowie **Jadc2s** 0.9.0 (und älter): Fehler beim Parsen von XML-Nachrichten, entfernter Angreifer kann beide Programme mit der Bytefolge 0xEF, 0xBB, 0xBF zum Absturz bringen. [http://www.securitytracker.com/alerts/2004/Sep/1011383.html]

Subversion: Zugriffskontrollfehler in »mod_authz_svn«, entfernter Angreifer erhält unberechtigt Zugriff auf Metadaten. [http://www.securitytracker.com/alerts/2004/Sep/1011390.html]

Cyrus SASL 2.1.19 und älter: Fehler beim Verarbeiten der »SASL_PATH«-Umgebungsvariable und Buffer Overflow in »digestmda5.c«, lokale und entfernte Angreifer können Befehle mit höheren Rechten ausführen. [http://www.securityfocus.com/bid/11347]

Freeradius 1.0.0: Fehler in »radius.c« und »eap_tls.c«, Denial-of-Service-Attacke möglich. [http://www.securityfocus.com/bid/11222]

GNU Radius vor 1.2.94: Integer Overflow in der »asn_decode_string()«-Funktion, entfernter Angreifer kann den Daemon zum Absturz bringen, wenn er mit »--enable-snmp« übersetzt wurde. [http://www.idefense.com/application/poi/display?id=141&type=vulnerabilities]