InSecurity News

Bugzilla

Die Bugzilla-Anwendung enthält mehrere Schwachstellen. Wenn der SQL-Server gestoppt wird, aber der Webserver weiterläuft, kann ein entfernter Angreifer die Datei »index.cgi« aufrufen und dadurch das Datenbank-Passwort erfahren. Betroffen sind die Versionen 2.17.1 bis 2.17.7. [http://bugzilla.mozilla.org/show_bug.cgi?id=227191]

Zudem findet sich ein Fehler in den Funktionen, mit denen Benutzer Mitgliedschaften an andere User weitergeben. Ein entfernter Angreifer kann Rechte auf Benutzergruppen übertragen, wozu er eigentlich keine Berechtigung hat. Betroffen sind die Versionen 2.17.1 bis 2.17.7. [http://bugzilla.mozilla.org/show_bug.cgi?id=233486]

Durch Fehler in »duplicates.cgi« und »buglist.cgi« kann ein entfernter Angreifer die Namen von Hidden Products lesen. Anfällig hierfür sind die Versionen vor 2.16.6 sowie die Version 2.18rc1. [http://bugzilla.mozilla.org/show_bug.cgi?id=234825] und [http://bugzilla.mozilla.org/show_bug.cgi?id=234855]

Ein entfernter Angreifer kann durch zahlreiche Eingabekontrollfehler in Skripten wie »editmilestones.cgi« erfolgreich Cross-Site-Skripting-Attacken durchführen. Betroffen sind die Ausgaben vor 2.16.6 sowie Version 2.18rc1. [http://bugzilla.mozilla.org/show_bug.cgi?id=235265]

Wenn ein entfernter Benutzer ein Chart ansieht, erscheint das Passwort in den Logdateien des Webservers. Das könnte ein lokaler Angreifer ausnutzen. Betroffen hiervon sind die Versionen 2.17.5 bis 2.17.7. [http://bugzilla.mozilla.org/show_bug.cgi?id=235510]

Ein Programmierfehler im »editusers.cgi«-Skript erlaubt es entfernten Angreifern, SQL-Injection-Attacken auszuführen. [http://bugzilla.mozilla.org/show_bug.cgi?id=244272] ■

Samba

In Samba wurden zwei Buffer-Overflows gefunden. Der erste betrifft SWAT (Samba Web Administration Tool), Versionen 3.0.2 bis 3.0.4. Ein entfernter Angreifer kann Befehle einschleusen, wenn er einen HTTP-Basic-Authentication-Header mit ungültigen Base64-Zeichen an das System schickt.

Ein weiterer Overflow findet sich in dem Samba-Programmteil, der die »mangling method = hash«-Option in der »smb.conf«-Datei verarbeitet. Betroffen hiervon sind die Versionen 3.0.0 und älter. [http://www.securitytracker.com/alerts/2004/Jul/1010753.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.	

Play-SMS

Im SMS-Gateway Play-SMS wurden mehrere Schwachstellen gefunden. Ein entfernter Angreifer kann Befehle mit den Rechten von Play-SMS ausführen. Eine zweite Sicherheitslücke erlaubt es ihm, SQL-Injection-Attacken durchzuführen. Durch geschickte SMS-Befehle kann er auch bestimmte Skripte auf dem System ausführen.
Betroffen hiervon sind die Versionen 0.6 und älter. [http://www.securitytracker.com/alerts/2004/Jul/1010738.html] ■

Tabelle 2: Linux-Advisories vom 18.07. bis 14.08.04

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

ID	Linux	Fehlerhafte Software
13956	Suse	PHP
13957	Debian	Ethereal
13959	Debian	Netkit-Telnetd-SSL
13961	Debian	L2tpd
13969	Red Hat	PHP
13970	Red Hat	PHP
13984	Red Hat	Libxml2
13985	Red Hat	WU-FTPD
13986	Red Hat	Sysklogd
13987	Red Hat	Mailman
13988	Debian	PHP
14004	Red Hat	Samba
14005	Mandrake	Samba
14006	Debian	Libapache-Mod-SSL
14007	Debian	Courier Sqwebmail
14008	Debian	Mailreader
14009	Suse	Samba
14030	Red Hat	Samba
14049	Mandrake	PostgreSQL ODBC-Treiber
14050	Mandrake	Webmin
14052	Mandrake	Xdm
14054	Debian	Libapache-Mod-SSL
14055	Mandrake	Mod-SSL
14059	Mandrake	Sox
14063	Red Hat	IPsec-Tools
14064	Red Hat	Sox
14065	Mandrake	WV
14066	Mandrake	Open-Office-Neon-Bibliothek
14085	Debian	Squirrelmail
14088	Generisch	Checkpoint VPN-1
14099	Generisch	Mozilla und Netscape
14100	Red Hat	Red-Hat-Linux-Kernel
14101	Red Hat	Red-Hat-Kernel
14111	Generisch	Libpng
14112	Suse	Libpng
14113	Debian	Libpng
14114	Red Hat	Libpng
14115	Mandrake	Libpng
14122	Red Hat	DNS-Resolver der Glibc
14123	Red Hat	Ethereal
14124	Generisch	Mozilla
14130	Suse	Linux-Kernel
14138	Mandrake	Shorewall
14160	Suse	Gaim
14162	Mandrake	Gaim
14163	Mandrake	Mozilla
14164	Generisch	Adobe Acrobat Reader

In Zusammenarbeit mit dem DFN-CER

PHP

Ist in PHP »memory_limit« aktiviert, kann ein entfernter Angreifer Befehle mit Webserver-Rechten ausführen. Eine HTTP-POST-Nachricht mit manipuliertem Header stört die Speicherallokation der Zend-Hashtabellen. Anschließend kann der Angreifer einen beliebigen Destruktor-Pointer für die Hashtabelle vorgeben und eigene Befehle ausführen. Betroffen sind die Versionen 4.3.7 (und älter) sowie 5.0.0RC3 (und älter). [http://security.e-matters.de/advisories/112004.html]
Eine weitere Schwachstelle steckt in der »strip_tags()«-Funktion. Ein entfernter Angreifer kann spezielle Tags einschleusen, die nur von einigen Browsern erkannt werden (darunter MS Internet Explorer und Apples Safari). Die Attacke ist nur möglich, falls »magic_quotes_gpc« deaktiviert ist. In diesem Fall übersieht die »strip_tags()«-Funktion Tags, die ein Null-Byte enthalten, zum Beispiel »<s\0cript>«.
Diese Browser sind unempfindlich gegen die Attacke: Opera, Konqueror, Mozilla, Firefox und Epiphany. Betroffen sind PHP 4.3.7 (und älter) sowie 5.0.0RC3 (und älter). [http://security.e-matters.de/advisories/122004.html] ■

Gnome VFS

In Extfs-Backend-Skripten für Gnome-VFS wurden Sicherheitslücken gefunden. Hierdurch kann ein entfernter Angreifer Befehle einschleusen. Er muss eine spezielle URL konstruieren. Öffnet sein Opfer diese mit Gnome VFS, dann führt der Angreifer Befehle mit den Rechten des Anwenders aus. [http://www.securityfocus.com/bid/10864] ■

Linux-Kernel

Aufgrund einer Schwachstelle in den Kernel-Funktionen »eql_g_slave_cfg()« und »eql_s_slave_cfg()« kann ein lokaler Angreifer den Kernel zum Absturz bringen. Die Programmierfehler liegen in der Datei »drivers/net/eql.c«. Bestätigt wurde dieser Fehler für Version 2.6.7. [http://www.securitytracker.com/alerts/2004/Jul/1010700.html]
Fehlerhaft ist auch das Handling der 64-Bit-Variante von Datei-Offset-Zeigern. Ein lokaler Angreifer erhält Einblick in Kernelspeicher.
Betroffen sind Linux 2.4 bis 2.4.26 sowie 2.6 bis 2.6.7. [http://isec.pl/vulnerabilities/isec-0016-procleaks.txt]
Durch einen weiteren Kernel-Bug kann ein lokaler Angreifer Gruppenrechte von Dateien ändern. Der Programmierfehler liegt im Syscall »sys_chown()«. Betroffen ist Version 2.4.27. [http://www.securitytracker.com/alerts/2004/Aug/1010859.html] ■

- Anzeige -

Kurzmeldungen

Shorewall vor 2.0.3a und 1.4.10f: Symlink-Fehler beim Verarbeiten von temporären Dateien und Verzeichnissen, lokaler Angreifer kann Dateien mit Root-Rechten überschreiben. [http://www.securityfocus.com/bid/10682]

Moodle 1.3.2+ stable, 1.4 dev: Eingabekontrollfehler im »help.php«-Skript, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2004/Jul/1010697.html]

PHP-BB vor 2.0.10: Eingabekontrollfehler, Cross-Site-Skripting möglich. [http://www.waraxe.us/index.php?modname=sa&id=34] und [http://www.securitytracker.com/alerts/2004/Jul/1010741.html]

Extropia Webstore: Eingabekontrollfehler in »web_store.cgi« bei »page«-Parameter, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/10744]

Cute News 1.3.x: Eingabekontrollfehler in »addcomment«-Funktion (»/inc/Shows.inc.php«-Skript), Cross-Site-Skripting möglich. [http://www.darkbicho.iberhosting.net/advisory-11.txt]

Nessus vor 2.0.12: Race-Condition-Fehler beim Handling der »TMPDIR«-Variablen, lokaler Angreifer kann höhere Rechte erlangen. [http://www.securityfocus.com/bid/10784]

Litecommerce 2.0.0: Zugriff auf Installationsskript »install.php« möglich, entfernter Angreifer kann administrativen Zugriff erlangen. [http://www.securitytracker.com/alerts/2004/Jul/1010778.html]

Opendocman vor 1.2: Authentifizierungsfehler in »commitchange.php«, entfernter, angemeldeter Angreifer kann Benutzer und Kategorien manipulieren. [http://www.securityfocus.com/bid/10807]

Phorum 5.0.7.beta: Eingabekontrollfehler in »search.php«, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/10822]

IBM Websphere 4.0.1, 4.0.2 und 4.0.3: Fehler beim Verarbeiten bestimmter HTTP-Header, entfernter Angreifer kann Websphere zum Absturz bringen. [http://www.securityfocus.com/bid/10651]

Power-Portal 1.3: Eingabekontrollfehler in »private_messages«-Modul, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/10835]

Antiboard 0.7.2 (und älter): Einige Eingabekontrollfehler in »antiboard.php«-Funktionen, Cross-Site-Skripting und SQL-Injection möglich. [http://www.securitytracker.com/alerts/2004/Jul/1010803.html]

Citadel/UX 6.23 (und älter): Buffer Overflow beim Verarbeiten des »USER«-Befehls, entfernter Angreifer kann Anwendung zum Absturz bringen. [http://www.nosystem.com.ar/advisories/advisory-04.txt]

Lost Book 1.1 (und älter): Eingabekontrollfehler in E-Mail- und Website-Feldern, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/10825]

LinPHA 0.9.4: Fehler in Cookie-Authentifizierungsmechanismus (»admin.php«), entfernter Angreifer kann administrativen Zugriff erlangen. [http://www.securityfocus.com/bid/10827]

IBM Directory Server 4.1 (und älter): Double-Dot-Schwachstelle in »ldacgi«-Skript, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.oliverkarow.de/research/IDS_directory_traversal.txt]

Squirrelmail 1.4.2 (und älter): Eingabekontrollfehler in »abook_database.php«-Skript (»alias«-Variable), SQL-Injection-Attacke möglich. [http://www.securitytracker.com/alerts/2004/Aug/1010842.html]

Rip-MIME vor 1.3.2.3: Fehler bei Base64-Dekodierung einiger Viren, entfernter Angreifer kann Viren trotz Antivirenprogramm einschleusen. [http://www.securityfocus.com/bid/10848]

Endonesia 8.3: Eingabekontrollfehler bei »query«-Variable, Cross-Site-Skripting möglich. [http://echo.or.id/adv/adv02-y3dips-2004.txt]

Sox

Beim Abspielen von WAV-Dateien mit Sox kann es zu einem Buffer Overflow kommen. Ein entfernter Angreifer kann dies ausnutzen, indem er eine manipulierte WAV-Datei an sein Opfer sendet. Beim Abspielen mit Sox führt das Opfer die Befehle des Angreifers aus. Die Buffer Overflows treten bei den Befehlen »sox« und »play« auf.
Der Programmierfehler liegt in der Funktion »st_wavstartread()« (in »wav.c«). Betroffen sind die Sox-Versionen 12.17.2 bis 12.17.4. [http://www.securityfocus.com/bid/10819] ■

WHM Autopilot

In WHM Autopilot kann ein entfernter Angreifer an Zugangsdaten von Benutzern gelangen. Das Informationsleck steckt in »clogin.php«. Der Angreifer muss diesem Skript einen speziellen Wert für die »c«-Variable übergeben, um an die Account-Informationen zu gelangen. Dieser Wert berechnet sich aus der User-ID. Betroffen ist die Version 2.4.5. [http://www.securityfocus.com/bid/10846] ■

Opera

In Opera kann ein entfernter Angreifer über eine HTML-Seite Dateien des Client-Systems lesen. Der Fehler geschieht beim Verarbeiten des »location«-Objekts. Betroffen sind die Versionen 7.53 und älter. [http://www.greymagic.com/security/advisories/gm008-op/] ■

GnuTLS

GnuTLS geht beim Verifizieren von X.509-Zertifikatsketten in einer ungünstigen Reihenfolge vor. So kann ein entfernter Angreifer erfolgreich eine Denial-of-Service-Attacke durchführen.
Statt beim Root-Zertifikat zu beginnen, startet GnuTLS für die Verifikation mit dem User-Zertifikat und hangelt sich bis zur Root-CA durch. Ein Angreifer kann daher beliebig manipulierte Schlüssel verwenden und damit Rechenleistung blockieren.
Würde GnuTLS beim Root-Zertifikat beginnen, könnte die Bibliothek ungültige und manipulierte Keys erkennen, bevor sie sie benutzt.
Betroffen sind die Versionen 1.0.16 und älter. [http://www.hornik.sk/SA/SA-20040802.txt] ■

Libpng

In der Libpng-Bibliothek wurden mehrere Buffer-Overflow-Fehler gefunden. Ein entfernter Angreifer kann Befehle mit den Rechten des Anwenders ausführen. Die Overflows treten bei manipulierten PNG-Dateien auf.
Zudem führen Integer Overflows dazu, dass ein entfernter Angreifer über eine spezielle PNG-Datei die Anwendung zum Absturz bringen kann. Betroffen sind die Versionen 1.2.5 und 1.0.15. [http://www.securitytracker.com/alerts/2004/Aug/1010854.html]
Weitere Overflows führen zu den gleichen Problemen. Betroffen sind Versionen vor 1.2.6rc1 und vor 1.0.16rc1. [http://www.securitytracker.com/alerts/2004/Aug/1010871.html] ■

OpenFTPD

In OpenFTPD kann ein entfernter, angemeldeter Angreifer Befehle mit den Rechten des FTP-Servers ausführen. Der Format-String-Fehler tritt auf, wenn sich FTP-Benutzer gegenseitig eine bestimmte Nachricht senden. Das funktioniert über den Befehl »site msg send *User-ID*«. Darin ist User-ID der Name des anderen FTP-Benutzers.
Der Programmierfehler liegt in »misc/msg.c«. Betroffen sind ProFTPD 0.30.2 (vor 16. Juli 2004) und ältere Versionen. [http://www.securityfocus.com/bid/10830] ■

Subversion

Eine Sicherheitslücke in Mod_authz_svn von Subversion führt dazu, dass ein entfernter, angemeldeter Angreifer unberechtigt Teile der verwalteten Daten ansehen kann. Voraussetzung ist aber, dass der Angreifer Schreibzugriff auf die Daten besitzt.
Mit Mod_authz_svn kopiert der Angreifer die Daten, die er lesen möchte, an eine Stelle, an der er Lesezugriff hat. Svnserve ist von diesem Fehler nicht betroffen. Anfällig ist Subversion 1.0.5 (und älter). [http://www.securityfocus.com/bid/10800] ■

Kurzmeldungen

Goscript 2.0: Eingabekontrollfehler in »go.cgi«, entfernter Angreifer kann Befehle mit den Rechten des Webservers ausführen. [http://www.securityfocus.com/bid/10853]

Gaim: Buffer Overflow beim Verarbeiten des MSN-Protokolls, entfernter Angreifer kann Befehle auf Client-System ausführen. [http://www.securityfocus.com/bid/10865]

CVS-Trac 1.1.3: Eingabekontrollfehler, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securitytracker.com/alerts/2004/Aug/1010880.html]

PureFTPD vor 1.0.19: Stürzt ab, sobald die Höchstzahl an Verbindungen erreicht ist, Denial of Service möglich. [http://www.securityfocus.com/bid/10664]

PHP-Nuke: Eingabekontrollfehler in »modules/Search/index.php«, SQL-Injection und Cross-Site-Skripting möglich. [http://www.waraxe.us/index.php?modname=sa&id=35] und [http://www.securitytracker.com/alerts/2004/Jul/1010734.html]

Dropbear SSH-Server 0.43: Fehler im Speichermanagement (benutzt »free()« für nicht initialisierte Variablen), entfernter Angreifer kann Befehle mit den Rechten des SSH-Daemon ausführen. [http://www.securityfocus.com/bid/10803]

Pavuk: Buffer Overflow beim Verarbeiten von Digest-Challenge-Feldern in HTTP-401-Nachrichten, entfernter Angreifer kann Befehle einschleusen. [http://www.securityfocus.com/bid/10797]

Myserver 0.6.2: Fehlerhafte Eingabekontrolle in »math_sum.mscgi«, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen, außerdem ist Cross-Site-Skripting möglich. [http://members.lycos.co.uk/r34ct/main/MyServer_0.6.2.txt]

Dansguardian 2.8 und älter: Eingabekontrollfehler, entfernter Angreifer kann den Dateinamen-Erweiterungs-Filter umgehen. [http://www.securityfocus.com/bid/10823]

Jaws 0.4: Eingabekontrollfehler in »controlpanel.php« falls »magic quotes« in »config.php« deaktiviert ist, SQL-Injection möglich. [http://www.securityfocus.com/bid/10826]

- Anzeige -

Checkpoint VPN-1

Ein Buffer Overflow in Checkpoint VPN-1 führt dazu, dass ein entfernter Angreifer Befehle einschleusen kann. Der Overflow tritt beim Verarbeiten von ASN.1-kodierten Werten in IKE-Pakete auf. [http://www.securitytracker.com/alerts/2004/Jul/1010798.html]
Die gleiche Schwachstelle hat auch Provider-1. [http://www.securitytracker.com/alerts/2004/Jul/1010799.html] ■

Mod_ssl

Im Apache-Modul Mod_ssl wurde ein Format-String-Fehler gefunden. Ein entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen, wenn das System auch das Mod_proxy-Modul verwendet. Die Schwachstelle liegt in der »ssl_engine_ext.c«-Datei und tritt dort bei einer Fehlermeldung auf.
Betroffen sind die Versionen vor 2.8.19-1.3.31. [http://www.securityfocus.com/bid/10736] ■

Neue Releases

Scapy: Umfangreiches Programm zur Manipulation von Netzwerkpaketen. [http://www.secdev.org/projects/scapy]

Lyceum: Backdoor mit eingebauter Verschlüsselung. [http://packetstormsecurity.org/UNIX/penetration/rootkits/lyceum-2.46.tar.gz]

Port Knocking: Kurze Einführung in die Port-Knocking-Technologie. [http://home.ripway.com/2004-5/110817/PortKnocking.php]

Fwknop: Port-Knocking-Implementierung, die auf IPtables basiert. [http://www.cipherdyne.org/fwknop/]

Putty

Im SSH-Client Putty wurde eine Sicherheitslücke entdeckt. Ein entfernter Angreifer braucht dazu die Kontrolle über einen SSH-Server, auf den sich sein Opfer mit Putty einloggt. Er kann dann auf dem Client-System Befehle mit den Rechten des Putty-Anwenders ausführen. Der Bug tritt schon vor der Anmeldung auf, bei SSH 2 lässt er sich bereits vor der Host-Verifikation nutzen. Betroffen sind die Versionen vor 0.55. [http://www.securitytracker.com/alerts/2004/Aug/1010849.html] ■

Postnuke

Unter Umständen kann ein entfernter Angreifer den Benutzernamen und das Passwort des Postnuke-Admin erfahren. Auf zahlreichen Systemen wurde »install.php« nach der Installation nicht entfernt. Ein Angreifer kann diese Datei abrufen und darin die Accountdaten sehen. Betroffen davon sind die Versionen 0.73x bis 0.75 GOLD. [http://www.securitytracker.com/alerts/2004/Jul/1010755.html]
Ein Eingabekontrollfehler in »showcontent()« ermöglicht Cross-Site-Skripting. Betroffen sind die Versionen 0.75-RC3 und 0.726-3. [http://www.securitytracker.com/alerts/2004/Jul/1010733.html]
In dem Easyweb-Dateimanager kann ein entfernter Angreifer Dateien mit Webserver-Rechten lesen. Er nutzt dazu die Double-Dot-Fehler der »pathext«- und »view«-Variablen in Postnuke 1.0 RC-1. [http://www.cirt.net/advisories/ew_file_manager.shtml] ■

Mozilla

Ein entfernter Angreifer kann ein ungültiges Root-CA-Zertifikat unauffällig in den Mozilla seines Opfers importieren. Dies führt zu einer Denial-of-Service-Attacke, da das falsche Zertifikat die gültigen Root-CA-Zertifikate im Browser überschreibt. Der Benutzer erhält den Fehlercode »-8182« (ungültiges Zertifikat), wenn er eine HTTPS-Verbindung öffnet.

Listing 1: Firefox-Exploit

```
01 <HTML><HEAD>
02 <TITLE>Faelschung</TITLE>
03 <META HTTP-EQUIV="REFRESH" CONTENT="0;
   URL=<I>https://www.example.com<I>">
04 </HEAD><BODY
05 onunload="
06 document.close();
07 document.writeln('<body onload=document.
   close();break;>
08 <h3>Wir verwenden das example.com-
   Zertifikat');
09 document.close();
10 window.location.reload();
11 "></BODY>
```

Um das ungültige Zertifikat zu importieren, muss der Angreifer eine spezielle Mail mit MIME-Typ »application/x-x 509-email-cert« an sein Opfer schicken. Die Mozilla-Mail-Komponente importiert das falsche Zertifikat direkt in den Personal Security Manager. Ein Angriff ohne Mail direkt über eine Website ist ebenfalls möglich. Hierzu muss der Angreifer eine Seite mit speziellen »IFRAME«-Tags anlegen. Betroffen sind die Versionen 1.7 und älter. [http://www.securitytracker.com/alerts/2004/Jul/1010714.html]

Ein weiteres Zertifikat-Problem wurde in der Mozilla-Browser-Variante Firefox gefunden. Ein Angreifer kann eine HTML-Seite schreiben, die das Zertifikat einer beliebigen anderen Website verwendet. Die Attacke nutzt Sicherheitslücken in den Meta-Refresh-Tags, siehe **Listing 1**. Firefox meldet dem Benutzer, dass sich die Seite mit dem Zertifikat der Domain »www.example.de« korrekt authentifiziert habe und verschlüsselt übertragen wurde. Dennoch stammt ihr Inhalt vom Angreifer, der einen anderen Server benutzt. Betroffen hiervon sind die Versionen 0.9.1 und 0.9.2. [http://www.securitytracker.com/alerts/2004/Jul/1010774.html]

Außerdem findet sich in Mozilla ein Integer Overflow beim Verarbeiten von SOAP-XML-Parametern. Ein entfernter Angreifer kann dadurch eine HTML-Seite anlegen, die beliebige Befehle mit den Rechten des Mozilla-Anwenders ausführt. Betroffen hiervon sind die Versionen 1.7 und älter. [http://www.idefense.com/application/poi/display?id=117&type=vulnerabilities]

(M. Vogelsberger/fjl) ■

- Anzeige -