# InSecurity News

## Zebra und Quagga

Durch eine Schwachstelle in Zebra kann ein entfernter Angreifer das Programm zum Absturz bringen. Das Problem tritt auf, wenn das Passwort-Feature aktiviert ist. Der Angreifer öffnet eine Telnet-Verbindung zum Management-Port und sendet bestimmte Daten, die dann zum Absturz führen. Betroffen ist Version 0.93b. [http://www.securitytracker.com/alerts/2003/Nov/1008189.html]

Ein ähnliches Problem wurde in Quagga, dem Zebra-Nachfolger, gefunden. Betroffen sind die Versionen vor 0.96.4. [http://www.securitytracker.com/alerts/2003/Nov/1008190.html] ■

## SAP-Datenbank

Ein Sicherheitsproblem in der SAP-Datenbank hat zur Folge, dass ein entfernter Angreifer Befehle auf dem System ausführen kann. Er erhält dabei Root- oder Local-System-Rechte. Die Schwachstelle liegt im »niserver«-Interface, es handelt sich um einen Buffer Overflow in der Funktion »eo420_GetStringFromVarPart()« (»sys/src/eo/veo420.c«). Ein Angreifer kann sie ausnutzen, indem er spezielle Daten an den TCP-Port 7269 schickt.

Betroffen davon sind die Versionen 7.4.03.27 und älter. [http://www.securitytracker.com/alerts/2003/Nov/1008207.html]

Auch einige Webtools der SAP-Datenbank weisen diverse Schwachstellen auf. Sie sind anfällig für Double-Dot-Fehler. Ein entfernter Angreifer kann Dateien mit Webserver-Rechten lesen. Dem Angreifer gelingt es auch, Zugang zu den Administrationsseiten des Web-Agenten zu erlangen, ohne sich vorher zu authentifizieren. Ein Buffer-Overflow-Fehler im Administrationsservice für den Web-Agenten lässt sich ebenfalls ausnutzen.

Ein weiterer Overflow findet sich im Programm »waecho« (Datei »vwd83echo.c«). Der Web-Datenbankmanager verwendet URL-basierte Session-IDs. Deren Wert ist aber nicht ausreichend zufällig, ein Angreifer kann ihn vorhersagen. Damit stellen sie keinen sicheren Schutz dar.

Aufgrund einer ungünstigen Konfiguration sind zahlreiche Dienste des Web-Agenten aktiviert. Die »websql«- und »webdbm«-Dienste führen dazu, dass ein entfernter Angreifer eventuell sogar die Möglichkeit erhält, auch an interne Datenbanken zu gelangen.

Betroffen davon sind die SAP-DB-Versionen vor 7.4.03.30. [http://www.atstake.com/research/advisories/2003/a111703-2.txt] ■

**Tabelle 1: Sicherheit bei den großen Distributionen**

| Distributor | Quellen zur Sicherheit | Bemerkungen |
|---|---|---|
| Debian | Infos: [http://www.debian.org/security/]<br>Liste: [http://lists.debian.org/debian-security-announce/]<br>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/]<br>Liste: [http://www.gentoo.org/main/en/lists.xml] (gentoo-announce und gentoo-security)<br>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]<br>Liste: [http://www.mandrakesecure.net/en/mlist.php] (announce)<br>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/]<br>Liste: [http://www.redhat.com/mailing-lists/] (redhat-watch-list)<br>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/]<br>Liste: [http://www.slackware.com/lists/] (slackware-security)<br>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/]<br>Patches: [http://www.suse.de/de/support/download/updates/]<br>Liste: suse-security-announce<br>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.

## BEA Weblogic Server und Express

Durch eine Denial-of-Service-Schwachstelle kann ein entfernter Angreifer das Proxy-Plugin von Weblogic Server und Express zum Absturz bringen. Um die Attacke auszuführen, muss der Angreifer geschickt formulierte URLs über den Proxy an Weblogic schicken. Betroffen sind Server und Express in den Versionen 6.1, 7.0 und 8.1. Zusätzlich muss das Proxy-Plugin verwendet werden (für Apache, I-Planet oder IIS). [http://www.securitytracker.com/alerts/2003/Nov/1008156.html]

Ein weiteres Problem in BEA Weblogic Server und Express betrifft den JMS-Provider (Java Messaging Service). Hierdurch sind lokale und entfernte Angreifer in der Lage, an das Passwort des Providers zu gelangen. Die BEA-Software speichert dieses Passwort als Klartext. Betroffen ist die Version 8.1. [http://www.securitytracker.com/alerts/2003/Nov/1008159.html]

Eine dritte Sicherheitslücke steht im Zusammenhang mit dem Einsatz des T3-Protokolls. Es kann vorkommen, dass Anwender, die eine verschlüsselte SSL-Verbindung verlangen, keine solche erhalten. Sollten sie dies nicht bemerken, übertragen sie eventuell geheime Daten abhörbar über das Netzwerk. Anfällig hierfür sind die Versionen 7.0, 7.0.0.1 und 8.1. [http://www.securitytracker.com/alerts/2003/Nov/1008160.html].

Ein entfernter Angreifer kann den Node Manager von Weblogic Server und Express zum Absturz bringen. Um die Attacke auszuführen, muss er nur einige spezielle Datenpakete an den Node-Manager-Port senden. Unter Umständen genügt dazu schon ein Portscan. Betroffen sind die Versionen 6.1, 7.0, 7.0.01 sowie 8.1. [http://www.securitytracker.com/alerts/2003/Nov/1008161.html]

Außerdem gelingt es einem entfernten Angreifer, die MBean-Konfiguration einzusehen. Dazu benötigt der Angreifer jedoch RMI-Zugang (Remote Method Invocation). Betroffen hiervon sind die Versionen 6.1, 7.0 und 8.1. [http://www.securitytracker.com/alerts/2003/Nov/1008162.html] ■

## Clam Antivirus

In Clam Antivirus (einem Virenscanner, der unter der GPL steht) wurde ein Format-String-Fehler entdeckt. Er führt dazu, dass ein entfernter Angreifer Befehle mit den Rechten des Clam-Benutzers oder (je nach Konfiguration) gar als Root ausführen kann. Zudem ist es ihm möglich, das Programm zum Absturz zu bringen.

Das Problem tritt an jener Codestelle in Clamav-Milter auf, die E-Mail-Absenderadressen per Syslog protokolliert. Es lässt sich nur ausnutzen, wenn die Syslog-Unterstützung in Clam enthalten ist, das gilt erst für Versionen nach 0.54. Ein entfernter Angreifer kann eigenen Code einschleusen, indem er eine E-Mail mit geschickt konstruiertem »From:«-Eintrag an das anfällige System schickt. Bestätigt wurde die Schwachstelle für die Versionen 0.60 bis 0.60p. [http://www.securityfocus.com/bid/9031] ■

## PHP-Coolfile

Aufgrund einer Sicherheitslücke in PHP-Coolfile kann ein entfernter Angreifer das Administrator-Passwort erfahren und so Zugang zum System erlangen. Der Programmierfehler liegt im PHP-Skript »action.php«. Bei einigen Anweisungen (darunter »edit«, »copy«, »print_chmod«) verzichtet das Skript auf eine Authentifizierung.

Dadurch kann ein entfernter Angreifer unter anderem die Datei »config.php« einsehen und den Administrator-Account auslesen:

```
http://Zielhost/php-coolfile/➥
action.php?action=edit&file=➥
config.php
```

Diese URL nutzt diese Sicherheitslücke beim Handling der »edit«-Anweisungen: PHP-Coolfile lässt den Angreifer daraufhin die Datei »config.php« bearbeiten.

Betroffen ist die Version 1.4. [http://www.securityfocus.com/bid/9018] ■

## People-Tools

In People-Tools wurden zwei Fehler entdeckt. Durch den ersten kann ein entfernter Angreifer den Installationspfad des Gateway Administration Servlet erfahren. Dazu muss er nur fehlerhafte Werte in bestimmte HTML-Formulare eingeben. Eine zu aussagefreudige Fehlermeldung gibt ihm die gewünschte Information. Betroffen sind 8.20, 8.43 sowie ältere. [http://www.securitytracker.com/alerts/2003/Nov/1008176.html]

Ein weiteres Problem wurde im I-Client gefunden. Dadurch kann ein entfernter Angreifer Befehle mit Webserver-Rechten ausführen. Er muss zunächst eine Datei auf den Server laden, die er gerne ausführen möchte. Diese Datei liegt dann in einem Verzeichnis mit zufälligem Namen unterhalb des Webroot-Verzeichnisses. Um sie ausführen zu können, muss er ihre genau Position kennen. Da I-Client die Zufallszahlen aber anhand der Serverzeit konstruiert, sind die Zahl und damit auch das Verzeichnis mit vertretbarem Aufwand zu erraten.

Anfällig hierfür sind die Versionen 8.1x, 8.2x und 8.4x. [http://www.securitytracker.com/alerts/2003/Nov/1008177.html] ■

### Neue Releases

**Python Network Security Tools:** Ein Python-Modul mit Namen Pcapy (Packet Capturing mit Python) und zwei Programme: Impacket (Protokoll-Bibliothek) und Inline-Egg (Assembler-Code in Python einbetten). [http://oss.coresecurity.com]

**FICC** (File Integrity Command and Control): Management-Tool für mehrere Tripwire-Installationen. [http://www.firsttracks.net/ficc/overview.php]

**Valgrind:** Prüft Programme auf Mängel in der Speicherverwaltung. Diese Fehler können sicherheitsrelevant sein. [http://valgrind.kde.org]

## Minimalist

Aufgrund eines Fehler in Minimalist kann ein entfernter Angreifer Befehle mit den Rechten des »minimalist.pl«-Skripts ausführen. Der Bug liegt in der »getAuth()«-Funktion. Übergibt der Angreifer einen »authcode« mit Pipezeichen, führt Minimalist die darauf folgenden Befehle aus. Betroffen sind die Versionen vor 2.3(3.3). [http://www.securityfocus.com/bid/9049] ■

## Sircd

Durch einen Fehler im Smart-IRC-Daemon (Sircd) kann ein entfernter, angemeldeter Angreifer Operator-Rechte erlangen. Eine einfache Mode-Anweisung ist ausreichend: »MODE *Nick-Name* +o«. Der Programmierfehler steckt in der Datei »s_client.c«.
Von diesem Fehler sind die Versionen 0.5.2 und 0.5.3 betroffen. [http://www.securityfocus.com/bid/9097] ■

## Terminator-X

In Terminator-X (einem Realtime-Audio-Synthesizer) wurden zahlreiche Schwachstellen entdeckt. Es handelt sich um mehrere Buffer-Overflow- und Format-String-Probleme, sie verschaffen einem lokalen Angreifer Root-Rechte.
Zunächst enthalten die Routinen, die die Kommandozeilenparameter »-f« und »-r« verarbeiten, jeweils einen Buffer Overflow. Fehlerhaft sind die beiden Funktionen »load_tt_part()« und »get_rc_name()«. Ein weiterer Overflow tritt auf, wenn der Angreifer spezielle Daten in die Umgebungsvariable »LADSPA_PATH« schreibt. In der Funktion »tx_note()« wurde ein Format-String-Fehler gefunden, er betrifft ebenfalls den Kommandozeilenparameter »-f«.
Anfällig für all diese Sicherheitslücken zusammen ist die Version 3.8.1. [http://www.securitytracker.com/alerts/2003/Nov/1008168.html] ■

**Tabelle 2: Linux-Advisories vom 18.11.03 bis 14.12.03**

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

| ID | Linux | Beschreibung |
|---|---|---|
| 10776 | Debian | Schwachstelle im Linux-NFS-Utils-Paket |
| 10777 | Debian | Schwachstelle in Sendmail |
| 10778 | Debian | Schwachstelle in Webmin/Usermin |
| 10779 | Debian | Fehler im Key-Validation-Code in GnuPG |
| 10792 | Suse | Schwachstellen in Sane |
| 10799 | Mandrake | Schwachstelle in Glibc |
| 10822 | Debian | Server des Debian-Projekts kompromittiert |
| 10863 | Red Hat | Schwachstellen in XDM |
| 10878 | Red Hat | Schwachstellen in Stunnel |
| 10880 | Red Hat | Schwachstelle in Pan |
| 10881 | Red Hat | Schwachstelle in IProute |
| 10882 | Red Hat | Schwachstelle in EPIC4 |
| 10883 | Red Hat | Schwachstelle in EPIC4 |
| 10908 | Mandrake | Schwachstellen in Stunnel |
| 10920 | Red Hat | Schwachstellen in XFree86 |
| 10921 | Red Hat | Schwachstellen in XFree86 |
| 10927 | Generisch | Schwachstelle bei GPG El-Gamal-Schlüsseln |
| 10941 | Generisch | Denial-of-Service-Schwachstelle in BIND 8 |
| 10945 | Suse | Denial-of-Service-Schwachstelle in BIND 8 |
| 10981 | Mandrake | Schwachstelle bei GPG El-Gamal-Schlüsseln |
| 10995 | Debian | Lokale Schwachstelle im Linux-Kernel 2.4 |
| 10996 | Mandrake | Lokale Schwachstelle im Linux-Kernel 2.4 |
| 11002 | Red Hat | Lokale Schwachstelle im Linux-Kernel 2.4 |
| 11014 | Red Hat | Schwachstelle in Net-SNMP |
| 11017 | Suse | Zwei Schwachstellen in GPG |
| 11036 | Suse | Lokale Schwachstelle im Linux-Kernel 2.4.X |
| 11043 | Debian | Heap Overflow in Rsync |
| 11044 | Suse | Heap Overflow in Rsync |
| 11045 | Red Hat | Heap Overflow in Rsync |
| 11046 | Mandrake | Heap Overflow in Rsync |
| 11049 | Suse | Support für Suse 7.3 wird eingestellt |
| 11095 | Mandrake | Schwachstelle in CVS-Server |
| 11096 | Mandrake | Schwachstelle in Screen |
| 11134 | Red Hat | Schwachstellen in GPG |
| 11135 | Mandrake | Schwachstelle in Ethereal |
| 11136 | Mandrake | Update: Schwachstelle in CVS-Server |

In Zusammenarbeit mit dem DFN-CERT

## Free Radius

Aufgrund einer Schwachstellen in Free Radius kann ein entfernter Angreifer den Server zum Absturz bringen. Dazu benötigt er zwar eine vom Server zugelassene IP-Adresse, die muss er aber nicht selbst besitzen. Per IP-Spoofing kann er sie beliebig fälschen. Der Programmierfehler führt zu einem Heap Overflow in einem Aufruf der Funktion »memcpy()«. Sendet der Angreifer ein String-Tag nach RFC 2868 mit zwei bis drei Oktetts Länge, ruft Free Radius die »memcpy()«-Funktion mit negativem Längenargument auf.
Betroffen sind die Versionen vor 0.9.3. [http://www.securityfocus.com/bid/9079] ■

## Prime Base SQL

Eine Sicherheitslücke in dem SQL-Datenbankserver Prime Base erlaubt es einem lokalen Angreifer, das Admin-Passwort der Datenbank zu sehen. Es ist als Klartext in der Datei »password.adm« abgelegt. Das Problem dabei: Das System ist so konfiguriert, dass jeder lokale Benutzer die Datei lesen kann.
Anfällig für diese Schwachstelle ist die Version 4.2. [http://www.securityfocus.com/bid/9087] ■

## Linux-Kernel 2.4

Im Kernel 2.4 führt ein Integer-Overflow-Problem dazu, dass lokale Angreifer Root-Rechte erlangen können. Die Sicherheitslücke verbirgt sich in der »do_brk()«-Funktion, die User-Programmen Zugriff auf den Kernel-Adressraum gestattet.
Ein Exploit findet sich bereits unter [http://packetstormsecurity.nl/0312-exploits/brk_poc.asm].
Betroffen sind die Kernel 2.4 bis 2.4.22. [http://www.securityfocus.com/bid/9138] ■

## Glibc, IProute und Zebra

Ein Programmierfehler in der »getifaddrs()«-Funktion der Glibc-Bibliothek führt dazu, dass lokale Angreifer einen Denial of Service erfolgreich durchführen können. Das Netlink-Interface des Kernels nimmt gefälschte Nachrichten an, die ein lokaler Anwender gesendet hat. Da »getifaddrs()« dieses Interface verwendet, sind alle Anwendungen betroffen, die jene Bibliotheksfunktion verwenden. Anfällig ist die Glibc-Version 2.3.2. [http://www.securitytracker.com/alerts/2003/Nov/1008170.html]

IProute ist ebenfalls von dem Netlink-Problem betroffen. [http://www.securitytracker.com/alerts/2003/Nov/1008173.html]

Auch die Zebra-Anwendung (Version 0.93b) ist anfällig. [http://www.securitytracker.com/alerts/2003/Nov/1008191.html] ■

## RNN Guestbook

In RNN Guestbook wurden mehrere Schwachstellen entdeckt. Mit Hilfe eines Fehlers im Skript »gbadmin.cgi« gelingt es einem entfernten Angreifer, ohne Anmeldung administrative Funktionen auszuführen. Außerdem kann er durch Programmierfehler in »gbadmin.cgi« auch Dateien mit Webserver-Rechten lesen. Ein angemeldeter Angreifer kann durch einen Eingabekontrollfehler bei der Pfadangabe der Gästebucheinträge Befehle ausführen. Cross-Site-Skripting-Attacken sind aufgrund einiger Sicherheitslücken im »guestbook.cgi«-Skript ebenfalls möglich.

Betroffen von diesen Problemen ist die Version 1.2. [http://www.securitytracker.com/alerts/2003/Nov/1008322.html] ■

## GnuPG

Durch eine Schwachstelle in den GnuPG-Routinen, die El-Gamal-Schlüssel erzeugen, kann ein entfernter Angreifer bestimmte private Schlüssel herausfinden. Zu der Sicherheitslücke kam es, als die GnuPG-Entwickler in Version 1.0.2 die Effizienz der El-Gamal-Verschlüsselung optimierten. Einem Angreifer genügt nun bereits eine Signatur, die mit einem dieser Keys erzeugt wurde, um den privaten Schlüssel zu bestimmen. Eine solche Signatur findet sich unter anderem in den selbst signierten öffentlichen Schlüsseln, die per Key-Server verteilt werden.

Das Problem betrifft allerdings nur die sehr seltenen El-Gamal-Schlüssel, die sowohl zum Verschlüsseln als auch zum Signieren verwendet werden (Typ 20). Die üblichen Schlüssel vom Typ 16 (nur Verschlüsselung) sind nicht betroffen. Um Typ-20-Schlüssel überhaupt erzeugen zu können, müssen GnuPG-Anwender ihr Programm mit speziellen Optionen übersetzt haben. Wer einen solchen Key besitzt, sollte ihn zurückrufen.

Das Problem findet sich in allen Versionen ab 1.0.2. [http://www.securitytracker.com/alerts/2003/Nov/1008319.html]

Außerdem wurde ein Format-String-Fehler im Programm »gpgkeys_hkp« gefunden. Ein Angreifer, der Kontrolle über einen Keyserver ausübt, kann damit Befehle auf dem Client-System ausführen. Der Programmierfehler liegt in der »get_key()«-Funktion (»keyserver/gpgkeys_hkp.c«). Dort findet sich ein »fprintf()«-Aufruf mit Benutzereingaben als Format-String.

Die Attacke gelingt nur über das HKP-Interface. In der stabilen Version 1.2 ist dies standardmäßig nicht aktiviert, in der Entwicklerversion 1.3 jedoch schon. Betroffen sind die Versionen 1.2.3 und 1.3.3. [http://www.securitytracker.com/alerts/2003/Dec/1008371.html] ■

## Screen

Ein Fehler in GNU Screen führt dazu, dass ein lokaler Angreifer Befehle mit Screen-Rechten ausführen kann. Je nach Installation sind dies Root-User- oder Utmp-Gruppenrechte.
Ein Angreifer muss dazu 2 bis 3 GByte Daten an einen Screen schicken, um einen Fehler in »ansi.c« auszunutzen. Es handelt sich um einen Integer Overflow der Variablen »w_NumArgs«.
Anfällig für den Overflow sind die Versionen 4.0.1, 3.9.15 und älter. [http://www.securityfocus.com/bid/9117]

## Monit

Im Monit-Daemon wurden gleich mehrere Fehler in der Speicherverwaltung entdeckt, durch die ein entfernter Angreifer Root-Rechte erlangen kann. Monit ist eine Web-basierte Host- und Netzwerk-Monitoring-Software. Um einen Overflow auszulösen, schickt der Angreifer eine geschickt konstruierte HTTP-Anfrage an den Server.
Zudem macht Monit einen Fehler bei dem Aufruf von »xmalloc()«: Übergibt ein Angreifer in einer HTTP-Anfrage einen negativen Content-Length-Wert, führt dies zum Absturz des Servers.
Betroffen von beiden ist die Version 4.1. [http://www.securitytracker.com/alerts/2003/Nov/1008290.html] ■

## OpenCA

In OpenCA (siehe auch PKI-Artikel in diesem Heft) wurden mehrere Sicherheitslücken entdeckt. Sie betreffen die RBAC-Zugangskontrolle (Role Based Access Control) mit digitalen Signaturen. OpenCA setzt sie zur Client-Authentifizierung auf der CA und der RA ein.
Durch den Bug kann es dazu kommen, dass OpenCA auch ungültige und abgelaufene Zertifikate annimmt und dem Client damit Administrator-Rechte gibt. Die Schwachstellen liegen in der Bibliothek »crypto-utils.lib« und treten bei »OpenCA::PKCS7« auf. Betroffen sind die Versionen 0.9.1.3 und älter. [http://www.securitytracker.com/alerts/2003/Nov/1008326.html] ■

## Ebola

In der Antivirus-Anwendung Ebola wurde ein Buffer-Overflow-Fehler entdeckt, durch den ein entfernter Angreifer Befehle mit den Rechten des Ebola-Servers ausführen kann. Der Overflow tritt im Ebola-Daemon (»ebola.c«) bei der Authentifizierung auf. Der Angreifer muss nur einen speziellen Benutzernamen angeben, er führt zum Overflow in der Funktion »handle_PASS()«.
Betroffen ist Version 0.1.4. [http://www.securitytracker.com/alerts/2003/Dec/1008396.html]
*(M. Vogelsberger/fjl)*

## Kurzmeldungen

**Monopd** vor 0.8.3: Race-Condition-Fehler, entfernter Angreifer kann Denial-of-Service-Attacke durchführen. [http://www.securityfocus.com/bid/9048]

**I-Planet-Webserver:** Fehler im Log-Analyzer beim Verarbeiten bestimmter Hostnamen, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2003/Nov/1008208.html]

**Omega-RPG** 0.90: Buffer Overflow bei Kommandozeilenparametern und Umgebungsvariablen, lokaler Angreifer kann Befehle mit Games-Rechten ausführen. [http://www.securityfocus.com/bid/9016]

**Pan-Newsreader** 0.13.3.93 (und älter): Fehler beim Verarbeiten von Nachrichten-Headern, entfernter Angreifer kann Client durch geschickt manipulierte Nachricht zum Absturz bringen. [http://www.securitytracker.com/alerts/2003/Nov/1008285.html]

**Bind** 8.4.2 (und älter): Fehler beim Verarbeiten ungültiger DNS-Antworten, entfernter Angreifer kann Denial-of-Service-Attacke durchführen. [http://www.securityfocus.com/bid/9114]

**PHP BB** 2.06: Eingabekontrollfehler im »search.php«-Skript, entfernter Angreifer kann SQL-Injection-Attacke durchführen. [http://www.securityfocus.com/bid/9122]

**Apache Mod_python:** Fehler beim Verarbeiten von Anfrage-Strings, entfernter Angreifer kann den Apache-Server zum Absturz bringen. [http://www.securityfocus.com/bid/9129]

**Jason Maloney Guestbook** 3.0: Verarbeitet »POST«-Daten nicht ordentlich, entfernter Angreifer kann Befehle mit Webserver-Rechten ausführen. [http://www.securityfocus.com/bid/9139]

**IBM Tivoli Directory Server** 4.1: Fehler beim Verarbeiten benutzerdefinierter Daten, Cross-Site-Skripting möglich. [http://www.securitytracker.com/alerts/2003/Dec/1008358.html]

**Sun-One-Webserver** 4.1 SP12 und älter sowie 6.0 SP5 und älter: Entfernter Angreifer kann Server zum Absturz bringen. [http://www.securitytracker.com/alerts/2003/Dec/1008364.html]

**Websense** 4.3.0 bis 5.1: Fehler beim Anzeigen blockierter URLs, Cross-Site-Skripting möglich. [http://www.securityfocus.com/bid/9149]

**Four in a Row (4inarow):** Fehler beim Verarbeiten der »PATH«-Variablen, lokaler Angreifer kann Befehle mit 4inarow-Rechten ausführen. [http://www.securitytracker.com/alerts/2003/Dec/1008395.html]

**Opera** 7.22 und älter: Buffer Overflow beim Laden von Skin-Dateien, entfernter Angreifer kann Befehle mit den Rechten des Opera-Anwenders ausführen. [http://www.securityfocus.com/bid/9089]

**PHP-Web-Filemanager** vor 2.0.2: Double-Dot-Schwachstelle, entfernter Angreifer kann Dateien des Systems mit Webserver-Rechten lesen. [http://www.securityfocus.com/bid/9053]

**Halflife-Server:** Wenn der Server Downloads erlaubt (»allowdownload=1«), sind eine Denial-of-Service-Attacke oder der Einblick in Konfigurationsdaten möglich. [http://www.securityfocus.com/bid/9070]

**Snif** vor 1.2.5: Das »index.php«-Skript kontrolliert die »download«-Variable nicht, entfernter Angreifer kann beliebige Dateien mit Webserver-Rechten herunterladen. [http://www.securityfocus.com/bid/9121]

**Rsync** 2.5.6 und älter: Fehler beim Verarbeiten von Daten auf Port 873, entfernter Angreifer kann Befehle mit Rsync-Rechten ausführen. [http://www.securitytracker.com/alerts/2003/Dec/1008380.html]

**X-Board** 4.2.6 und älter: Symlink-Schwachstelle in »pxboard«, lokaler Angreifer kann Dateien mit den Rechten von X-Board modifizieren. [http://www.securityfocus.com/bid/9151]

**SQ-Webmail:** Session-Hijacking-Schwachstelle, entfernter Angreifer kann die Sessions anderer Benutzer übernehmen. [http://www.securityfocus.com/bid/9058]

**Applied Watch Command Center** vor 1.4.5: Authentifizierung funktioniert für einige Nachrichten nicht, entfernter Angreifer kann neue Benutzer und zusätzliche IDS-Regeln hinzufügen. [http://www.securityfocus.com/bid/9124]