

# SecurityFocus Microsoft Newsletter #135

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-04/0105.html>

---

**From:** Marc Fossi ([mfossi\\_at\\_securityfocus.com](mailto:mfossi_at_securityfocus.com))

**Date:** 04/28/03

Date: Mon, 28 Apr 2003 14:31:29 -0600 (MDT)

To: Focus-MS <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>

SecurityFocus Microsoft Newsletter #135

---

This issue is sponsored by: FastTrain

FastTrain has your solution for a great CISSP Boot Camp. The industry's most recognized corporate security certification track, provides a comprehensive prospectus based upon the core principle concepts of security. This ALL INCLUSIVE curriculum utilizes lectures, case studies and true hands-on utilization of pertinent security tools. For a limited time you can enter for a chance to win one of the latest technological innovations, the SEGWAY HT.

Log onto <http://www.fasttraincamp.com>.

---

## I. FRONT AND CENTER

1. Auditing Web Site Authentication
2. Anti-Virus Defence In Depth
3. Al-Jazeera, the First Amendment, and Security Professionals
4. Secure by Default
5. SecurityFocus DPP Program

## II. MICROSOFT VULNERABILITY SUMMARY

1. Rinetd Connection List Resizing Denial of Service Vulnerability
2. Microsoft Windows SMB NTLM Authentication Interception...
3. 360 Degree Web PlatinumKey Access Control Bypass Application...
4. Xeneo Web Server Denial Of Service Vulnerability
5. YaBB SE Language Remote File Include Vulnerability
6. OpenBB Index.PHP Remote SQL Injection Vulnerability
7. EZ Server File Disclosure Vulnerability
8. Microsoft Windows Service Control Manager Race Condition...
9. PT News Unauthorized Administrative Access Vulnerability
10. OpenBB Board.PHP Remote SQL Injection Vulnerability
11. SAP Database Development Tools INSTDBMSRV INSTROOT Environment...
12. Snitz Forums 2000 Cross Site Scripting Vulnerability
13. Microsoft Internet Explorer CLASSID Variant Denial Of Service...
14. Working Resources BadBlue Ext.DLL Command Execution Vulnerability

15. MPCSoftWeb Guest Book HTML Injection Vulnerability
16. MPCSoftWeb Database Disclosure Vulnerability
17. 360 Degree Web PlatinumKey Access Control Bypass Information...
18. SAP Database Development Tools INSTLSERVER INSTROOT...
19. AN HTTPD Count.pl Directory Traversal Vulnerability
20. Microsoft Shlwapi.dll Malformed HTML Form Tag Denial of...
21. OpenBB Member.PHP Remote SQL Injection Vulnerability

### III. MICROSOFT FOCUS LIST SUMMARY

1. Article Announcement: Auditing Web Site Authentication (Thread)
2. Files in system 32 directory (Thread)
3. interoperability of VPN checkpoint FW1 to ISA (Thread)
4. Article Announcement: Anti-Virus Defence In Depth (Thread)
5. Auditing a reboot (Thread)
6. SecurityFocus Microsoft Newsletter #134 (Thread)
7. Does In-Place Upgrade of Microsoft Exchange Create Open...
8. Article Announcement: Statistical-Based Intrusion Detection...
9. checking server status (Thread)
10. Does In-Place Upgrade of Microsoft Exchange Create Open...

### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. EnterpriseSMS System 1
2. AppAudit
3. SiteRecorder

### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. cosign v1.0.0
2. pcInternet Patrol
3. WhiteHat Arsenal v1.05

### VI. SPONSOR INFORMATION

#### I. FRONT AND CENTER

---

1. Auditing Web Site Authentication  
By Mark Burnett

This is the first part of a two-part article discussing a standard audit procedure consisting of a list of questions to test Web site authentication schemes.

<http://www.securityfocus.com/infocus/1688>

2. Anti-Virus Defence In Depth  
by Ken Bechtel

Lately it seems I can't open my inbox with out seeing a new article on defence in depth. This is fine: defence in depth is crucial to anti-virus protection. Unfortunately, most of the articles are missing two crucial components. To understand what is being missed, we need to look at what is meant by defence in depth as it applies in the malicious software world. For the purpose of this paper, when referring to defence in depth, we will be specifically talking about the utilization of anti-virus software, and other methods to provide a multi-layered anti-malware defence in a corporate environment.

<http://www.securityfocus.com/infocus/1687>

### 3. Al-Jazeera, the First Amendment, and Security Professionals

By Scott Granneman

While attempts to disrupt Web broadcasts of Al-Jazeera may seem like a distant concern, they reflect the problems that should concern security professionals everywhere.

<http://www.securityfocus.com/columnists/156>

### 4. Secure by Default

By Tim Mullen

With Windows Server 2003, Microsoft has finally produced an operating system that isn't begging to be hacked on the first boot.

<http://www.securityfocus.com/columnists/157>

### 5. SecurityFocus DPP Program

Attention Universities!! Sign-up now for preferred pricing on the only global early-warning system for cyber attacks – SecurityFocus DeepSight Threat Management System.

Click here for more information:

<http://www.securityfocus.com/corporate/products/dpsection.shtml>

## II. BUGTRAQ SUMMARY

---

### 1. Rinetd Connection List Resizing Denial of Service Vulnerability

BugTraq ID: 7377

Remote: Yes

Date Published: Apr 17 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7377>

Summary:

rinetd is a small server designed to redirect connections from one IP address and port to another. It is available for the Microsoft Windows and Linux operating system.

By default rinetd allocates space for a list of 64 connections. When this 64-connection boundary has been reached, the program attempts to reallocate the buffer, to accommodate additional connections. A flaw has been discovered in the reallocation process that may open an opportunity for an attacker to trigger a denial of service.

Specifically, a buffer overflow may be triggered after attempting to reallocate memory. This is due to the buffer being reallocated incorrectly. As a result, when a new connection is established the

information will be written past the buffer. This may result in a segmentation violation and cause the process to crash.

It should be noted that, although unconfirmed, if data written passed the buffer can be controlled by an attacker it could be possible to exploit this issue to execute arbitrary code.

This vulnerability affects rinetd 0.61 and earlier.

## 2. Microsoft Windows SMB NTLM Authentication Interception Weakness

BugTraq ID: 7385

Remote: Yes

Date Published: Apr 19 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7385>

Summary:

Microsoft Windows uses the SMB protocol to authenticate against other Microsoft systems on a network.

A weakness has been reported whereby an attacker may be able to intercept SMB communications to access a vulnerable SMB client.

This weakness exists due to the way SMB connections are initiated. An attack would proceed by tricking a victim user to connect to an attacker-controlled server. The attacker's server would then send a request to an attacker-controlled client which initiates a request to a legitimate SMB server. The responses generated by the legitimate server would be relayed through the attacker-controlled systems to eventually gain control of the victim client.

Exploitation of this issue involves many specific scenarios and would be difficult. It has been reported that this issue is very similar to an attack described by DilDog presented at DefCon 2000.

## 3. 360 Degree Web PlatinumKey Access Control Bypass Application Execution Vulnerability

BugTraq ID: 7392

Remote: No

Date Published: Apr 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7392>

Summary:

PlatinumKey is a smart card security application distributed by 360 Degree Web. It is available for some laptops that use Microsoft Windows operating systems.

It has been reported that PlatinumKey does not properly restrict access to the desktop when smart card access control is enabled. Because of this, an attacker may be able to gain access to the task bar and potentially execute applications.

The problem is in the handling of certain key sequences. When the key sequence Control–Escape is pressed, the Windows task bar is displayed. An attacker could abuse this to gain access to the icons of recently run applications. By clicking on one of the applications stored in the frequently access applications menu, an attacker could execute the application.

It is unclear what privileges the application will be executed with during exploitation of this vulnerability. It is likely that the application will be executed with the privileges of the user whose session is locked.

This problem has been reported to occur on the Acer Travelmate 600 and 800 series laptops. It may additionally affect other laptops using the same software with similar configurations.

#### 4. Xeneo Web Server Denial Of Service Vulnerability

BugTraq ID: 7398

Remote: Yes

Date Published: Apr 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7398>

Summary:

Xeneo Web Server is a web server for Microsoft Windows platforms that supports ASP, PHP, ColdFusion, Perl, CGI and ISAPI.

Xeneo web server has been reported prone to Denial of Service vulnerability.

It has been reported that a malicious HTTP GET request containing over 4096 bytes of data will trigger this vulnerability. Specifically, an attacker may initiate a HTTP GET request including a "?" character followed by approximately 4096 bytes of data. This action will result in a denial of service condition triggered in the Xeneo web server.

Although absolutely unconfirmed, due to the nature of this vulnerability, memory corruption or arbitrary code execution may be possible.

It should also be noted, that although this vulnerability has been reported to affect Xeneo web server version 2.2.9.0 previous versions may also be vulnerable.

#### 5. YaBB SE Language Remote File Include Vulnerability

BugTraq ID: 7399

Remote: Yes

Date Published: Apr 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7399>

Summary:

YaBB SE is a freely available, open source port of Yet Another Bulletin Board (YaBB). It is available for a number of platforms include Unix, Linux, and Microsoft Windows operating systems.

YaBB may allow malicious bulletin board users to influence the include path for language files. Registered users may influence the include path of language files through the "Change Profile" option. A malicious user could set an include path that points to a malicious PHP script on an external host. This could result in execution of commands in the context of the web server.

#### 6. OpenBB Index.PHP Remote SQL Injection Vulnerability

BugTraq ID: 7401

Remote: Yes

Date Published: Apr 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7401>

Summary:

OpenBB is a freely available, open source bulletin board software package. It is available for Unix, Linux, and Microsoft Windows operating systems.

A problem with the software may make it possible for remote users to modify database query logic.

It has been reported that OpenBB does not properly check input passed via the 'index.php' script. Because of this, it may be possible for a remote user to inject malicious arbitrary SQL queries in the context of the database user for the bulletin board software. The consequences of successful exploitation will vary depending on the underlying database implementation, but may allow for disclosure of sensitive information or remote compromise of the bulletin board or database itself.

This vulnerability has been reported in OpenBB version 1.1.0. The currently available version reported by the vendor is 1.0.5. This vulnerability may affect the reported version, and previous versions of the affected software.

#### 7. EZ Server File Disclosure Vulnerability

BugTraq ID: 7378

Remote: Yes

Date Published: Apr 17 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7378>

Summary:

EZ Server is a freely available FTP and HTTP server. It is available for the Microsoft Operating System.

It has been announced that EZ Server is vulnerable to a condition that may result in the disclosure of potentially sensitive information.

According to the report, EZ Server does not perform correct validation on client requested paths which include "../" character sequences. It is possible for attackers to obtain files and directories outside of the webroot by requesting their path relative to the current directory using such sequences.

This may be exploited by a remote attacker to gain sensitive information useful in launching other attacks.

#### 8. Microsoft Windows Service Control Manager Race Condition Vulnerability

BugTraq ID: 7386

Remote: No

Date Published: Apr 20 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7386>

Summary:

A race condition error has been reported in the Microsoft Service Control Manager (SCM). The SCM manages and keeps track of installed services.

When the system is shutdown, the SCM may send a SERVICE\_CONTROL\_SHUTDOWN control code to service applications that are required to clean up before the system shutdown. The SCM will wait for service applications to shutdown for a specified time limit before continuing with the system shutdown. This condition could occur during system shutdown if services do not successfully shutdown within the specified time limit.

The race condition could cause random cached data to be included in files that are still open when the time limit expires for the service shutdown. In the worst case scenario, random sensitive data from administrative services could be included in output files for lower privileged services. This could expose sensitive data to local users with access to these output files. To exploit this condition, a malicious local user would need to monitor the output files after a reboot.

#### 9. PT News Unauthorized Administrative Access Vulnerability

BugTraq ID: 7394

Remote: Yes

Date Published: Apr 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7394>

Summary:

PT News is a web based news system. It is implemented in PHP and available for Microsoft Windows operating systems and Linux/Unix variants.

PT News does not adequately prevent remote users from gaining unauthorized access to administrative functions. The source of this issue is that the 'index.php' script includes the 'news.inc' file, which contains various administrative functions for PT News. Remote users may access the administrative functions of 'news.inc' through the 'index.php' script.

Exploitation could allow remote attackers to manipulate content.

#### 10. OpenBB Board.PHP Remote SQL Injection Vulnerability

BugTraq ID: 7404

Remote: Yes

Date Published: Apr 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7404>

Summary:

OpenBB is a freely available, open source bulletin board software package. It is available for Unix, Linux, and Microsoft Windows operating systems.

A problem with the software may make it possible for remote users to modify database query logic.

It has been reported that OpenBB does not properly check input passed via the 'board.php' script. Because of this, it may be possible for a remote user to inject malicious arbitrary SQL queries in the context of the database user for the bulletin board software. The consequences of successful exploitation will vary depending on the underlying database implementation, but may allow for disclosure of sensitive information or remote compromise of the bulletin board or database itself.

This vulnerability has been reported in OpenBB version 1.1.0. The currently available version reported by the vendor is 1.0.5. This vulnerability may affect the reported version, and previous versions of the affected software.

#### 11. SAP Database Development Tools INSTDBMSRV INSTROOT Environment Variable Vulnerability

BugTraq ID: 7407

Remote: No

Date Published: Apr 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7407>

Summary:

SAP DB is a free database software package for Unix, Linux, and Microsoft Operating Systems.

It has been reported that a vulnerability exists in the SAP Database program instdbmsrv. Because of this, a local attacker may be able to gain elevated privileges.

The problem is in the handling of input from untrusted sources. When executed, the instdbmsrv program checks the INSTROOT environment variable for the location of the pgm/dbmsrv program. The permissions of the dbmsrv program are changed to give the program setuid root privileges when the instdbmsrv is executed. An attacker could modify the INSTROOT environment variable locally to point to an arbitrary directory. When the instdbmsrv program is executed, an attacker-supplied version of the dbmsrv program

would be changed to setuid root.

This could result in an attacker gaining local administrative privileges.

#### 12. Snitz Forums 2000 Cross Site Scripting Vulnerability

BugTraq ID: 7381

Remote: Yes

Date Published: Apr 17 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7381>

Summary:

Snitz Forums 2000 is ASP-based web forum software. It runs on Microsoft Windows operating systems.

A cross site scripting vulnerability has been reported for Snitz Forums 2000.

The vulnerability exists due to insufficient sanitization of user-supplied values. Specifically, TAB characters are not properly sanitized from <IMG> tags.

This lack of sanitization provides an opportunity for an attacker to launch cross-site scripting attacks against the vulnerable site. It is possible for a remote attacker to create a malicious link containing script code that will be executed in the browser of a legitimate user.

Any attacker-supplied code will be executed within the context of the website running Snitz Forums 2000.

This issue may be exploited to steal cookie-based authentication credentials from legitimate users of the website running the vulnerable software. The attacker may hijack the session of the legitimate by using cookie-based authentication credentials. Other attacks are also possible.

#### 13. Microsoft Internet Explorer CLASSID Variant Denial Of Service Vulnerability

BugTraq ID: 7384

Remote: Yes

Date Published: Apr 18 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7384>

Summary:

Microsoft Internet Explorer contains a vulnerability that may allow for malicious webmasters to cause a victim user's web browser to stop responding.

A CLASSID is a unique identifier that provides information to the default COM handler. It is possible to include a CLASSID value as part of an OBJECT tag under some versions of Internet Explorer.

If a web page contains a specific CLASSID value and an IE user attempts to view the page, IE has been reported to crash. The reported offending CLASSID is CLSID:0CF32AA1-7571-11D0-93C4-00AA00A3DDEA, however there may be other CLASSID values which could exploit this issue.

This issue has been reported to occur when vulnerable versions of Internet Explorer are running under Windows 2000 or XP. It is not currently known if this issue is related to properties of the underlying operating system.

This vulnerability has been reported to affect Internet Explorer 6.0 SP1.

#### 14. Working Resources BadBlue Ext.DLL Command Execution Vulnerability

BugTraq ID: 7387

Remote: Yes

Date Published: Apr 20 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7387>

Summary:

BadBlue is a P2P file sharing application distributed by Working Resources. It is available for Microsoft Windows operating systems.

BadBlue is prone to a vulnerability that could allow remote attackers to gain unauthorized access. BadBlue includes a server-side scripting language which uses '.htx' and '.hts' files. The '.hts' extension represents files that are only intended to be requested and executed by the local host.

It has been reported that by inserting certain characters into a request for an '.hts' file, it is possible for a remote user to cause the '.hts' file to be interpreted by the server. This is due to an input validation error in the 'ext.dll' component, which is responsible for verifying the source of requests for '.hts' files. Exploitation could lead to unauthorized execution of administrative or restricted commands.

#### 15. MPCSoftWeb Guest Book HTML Injection Vulnerability

BugTraq ID: 7389

Remote: Yes

Date Published: Apr 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7389>

Summary:

MPCSoftWeb Guest Book is a web application for Microsoft Windows operating systems.

MPCSoftWeb Guest Book is prone to a vulnerability that could allow remote attackers to inject hostile HTML and script code into the guestbook system. The issue exists in the 'insertguest.asp' script. This is due to insufficient sanitization of guestbook form fields such as "Name", "location" and "comment". HTML and script code that is injected in this

manner may be interpreted in the web browser of users who visit the guestbook site. This will occur in the security context of the site hosting the guestbook software.

Successful exploitation may allow for theft of cookie-based authentication credentials or other attacks.

#### 16. MPCSoftWeb Database Disclosure Vulnerability

BugTraq ID: 7390

Remote: Yes

Date Published: Apr 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7390>

Summary:

MPCSoftWeb Guest Book is a web application for Microsoft Windows operating systems. It is backed by a Microsoft Access database.

MPCSoftWeb does not sufficiently secure the database file. This issue is due to lack of access controls to prevent remote users from requesting the database file. It is possible for remote attackers to request the database file and gain access to sensitive information such as administrative credentials for the guestbook.

#### 17. 360 Degree Web PlatinumKey Access Control Bypass Information Disclosure Vulnerability

BugTraq ID: 7391

Remote: No

Date Published: Apr 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7391>

Summary:

PlatinumKey is a smart card security application distributed by 360 Degree Web. It is available for some laptops that use Microsoft Windows operating systems.

It has been reported that PlatinumKey does not properly restrict access to the desktop when smart card access control is enabled. Because of this, an attacker may be able to gain access to potentially sensitive information.

The problem is in the handling of certain key sequences. When the key sequence Control-Escape is pressed, the Windows task bar is displayed. An attacker could abuse this to gain information about recently run applications and recently accessed documents.

This problem has been reported to occur on the Acer Travelmate 600 and 800 series laptops. It may additionally affect other laptops using the same software with similar configurations.

18. SAP Database Development Tools INSTLSERVER INSTROOT Environment Variable Vulnerability  
BugTraq ID: 7408

Remote: No

Date Published: Apr 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7408>

Summary:

SAP DB is a free database software package for Unix, Linux, and Microsoft Operating Systems.

It has been reported that a vulnerability exists in the SAP Database program instlserver. Because of this, a local attacker may be able to gain elevated privileges.

The problem is in the handling of input from untrusted sources. When executed, the instlserver program checks the INSTROOT environment variable for the location of the pgm/lserver program. The permissions of the lserver program are changed to give the program setuid root privileges when the instlserver is executed. An attacker could modify the INSTROOT environment variable locally to point to an arbitrary directory. When the instlserver program is executed, an attacker-supplied version of the lserver program would be changed to setuid root.

This could result in an attacker gaining local administrative privileges.

19. AN HTTPD Count.pl Directory Traversal Vulnerability

BugTraq ID: 7397

Remote: Yes

Date Published: Apr 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7397>

Summary:

AN HTTPD is a Web server designed for use on Microsoft Windows operating systems.

AN HTTPd contains a sample script named count.pl that may be used as a web counter. The script may accept a path and file name as arguments to store the numerical value of the counter.

This script does not perform adequate input validation on user-supplied paths containing directory traversal (../) character sequences. The vulnerable script may be used to overwrite any file on the system to which the 'CGI' user has write privileges, by supplying the file name and path in an HTTP request.

The 'CGI' user typically has System level privileges by default. As a result, an attacker may be capable of corrupting arbitrary system files.

20. Microsoft Shlwapi.dll Malformed HTML Form Tag Denial of Service Vulnerability

BugTraq ID: 7402

Remote: Yes

Date Published: Apr 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7402>

Summary:

The 'shlwapi.dll' is a dynamic link library that exports several shell functions. Several applications, such as Internet Explorer and Front Page use functions from this library when rendering HTML content.

When an HTML page containing a specifically malformed tag is rendered by an application that exports functions from 'shlwapi.dll', the host application will fail. It has been reported that this vulnerability could not be exploited to cause code execution.

The problem appears to be caused by an attempt to perform a case-insensitive comparison of two strings. Due to the malformed tag, one of these strings will be a null pointer. The result of this is that the comparison attempt causes an exception.

It has also been reported that an HTML page containing the malformed tag located on the local file system may cause explorer.exe to fail if the "Enable Web content in folders" option is selected.

21. OpenBB Member.PHP Remote SQL Injection Vulnerability

BugTraq ID: 7405

Remote: Yes

Date Published: Apr 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7405>

Summary:

OpenBB is a freely available, open source bulletin board software package. It is available for Unix, Linux, and Microsoft Windows operating systems.

A problem with the software may make it possible for remote users to modify database query logic.

It has been reported that OpenBB does not properly check input passed via the 'member.php' script. Because of this, it may be possible for a remote user to inject malicious arbitrary SQL queries in the context of the database user for the bulletin board software. The consequences of successful exploitation will vary depending on the underlying database implementation, but may allow for disclosure of sensitive information or remote compromise of the bulletin board or database itself.

This vulnerability has been reported in OpenBB version 1.1.0. The currently available version reported by the vendor is 1.0.5. This vulnerability may affect the reported version, and previous versions of

the affected software.

### III. MICROSOFT FOCUS LIST SUMMARY

-----

1. Article Announcement: Auditing Web Site Authentication (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/319605>

2. Files in system 32 directory (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/319564>

3. interoperability of VPN checkpoint FW1 to ISA (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/319537>

4. Article Announcement: Anti-Virus Defence In Depth (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/319467>

5. Auditing a reboot (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/319397>

6. SecurityFocus Microsoft Newsletter #134 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/319271>

7. Does In-Place Upgrade of Microsoft Exchange Create Open Relays? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/319274>

8. Article Announcement: Statistical-Based Intrusion Detection (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/319221>

9. checking server status (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/319199>

10. Does In-Place Upgrade of Microsoft Exchange Create Open Relays? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/319195>

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

---

##### 1. EnterpriseSMS System 1

by Integrated Command Software

Platforms: Windows NT

Relevant URL:

[http://www.commandsystems.com/system\\_1.html](http://www.commandsystems.com/system_1.html)

Summary:

The EnterpriseSMS System 1 is a single-user, single-CPU system designed to meet the needs of small system users. Running on Windows NT, and utilizing the industry-standard Oracle relational database, System 1 supports an unlimited number of readers and controllers, and is fully upgradeable to the largest EnterpriseSMS systems without functional changes to the software or database. Its feature set far exceeds that of comparably priced systems. ESMS System supports the Open System Controller. The Open System Controller utilizes FLASH RAM memory, which eliminates costly field service calls to change or update firmware. The Open System Controller is fully software-configurable. ESMS System 1 is field installable by either users or their dealers using an installation manager typical in the Windows environment. Simplified database templates make system configuration and system administration simple, even for the novice user. Remote diagnostics and complete support utilities are fully included with your EnterpriseSMS System 1/Open System Controller system.

##### 2. AppAudit

by Sanctum, Inc.

Platforms: N/A

Relevant URL:

<http://www.sanctuminc.com/solutions/appaudit/index.html>

Summary:

Sanctum's AppAudit will help you find the holes in your Web site before somebody else does. AppAudit is a remote audit on your Web site conducted by Sanctum, to determine the general security of your site at the application level. AppAudit reveals Web application vulnerabilities, including: Hidden Manipulation, Parameter Tampering, Cookie Poisoning, Stealth Commanding, Forceful Browsing, Backdoors and Debug options, Configuration Subversion, Buffer Overflow and Vendor-assisted Hacking.

##### 3. SiteRecorder

by LOCKSTEP SYSTEMS, INC.

Platforms: Windows 2000, Windows 95/98, Windows NT, Windows XP

Relevant URL:

<http://www.lockstep.com/products/siterecorder/sr-product.html>

Summary:

SiteRecorder goes beyond traditional backup by creating a revision history of your web site as it changes. Keeping a current backup copy of your web

site is ideal for disaster recovery – so you can restore the whole site or just fix a few mistakes. If you find a problem with the latest web site update, use SiteRecorder's Republish feature to quickly roll back your site to any previous version while corrections are made. As SiteRecorder backs up your site, it scans the content for any changes that have been made. When changes are detected, it automatically sends you an e-mail to keep you informed. Each e-mail includes a hyperlink list so you can quickly locate and view the new content.

## V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

### 1. cosign v1.0.0

by UMich Web Team

Relevant URL:

<http://weblogin.org/>

Platforms: UNIX, Windows 2000, Windows NT

Summary:

cosign is a Web single sign on system that allows users to authenticate once per session and access any protected Web resources at the institution. If used, passwords are sent only to a single, central URL. Sessions have both idle and hard timeouts, and users can logout of all protected services by visiting a single URL. The use of public key cryptography ensures that a compromise of a protected Web server has no impact on the security of other participating servers.

### 2. pcInternet Patrol

by Internet Security Alliance

Relevant URL:

<http://www.isa-llc.com/downloads/pcip.php>

Platforms: Windows 2000, Windows 95/98, Windows NT, Windows XP

Summary:

pcInternet Patrol maximizes protection with minimum user involvement. This product finds 6 times more potentially dangerous programs/modules than other leading personal firewalls. Other features are:

- Stops all intruder programs both known and unknown;
- Users always have the latest programs definition without the need for an update;
- Keeps you and your computer out of harms way, without getting in your way;
- Cannot be disabled by an intruder without alerting user or administrator;
- Activates Intruder tracking to trace IP address of intruder for possible apprehension;
- Continuously monitors the state of the NETBIOS ports, the first entry target for intruders;
- Help with security issues in real time!

3. WhiteHat Arsenal v1.05

by WhiteHat Security, Inc.

Relevant URL:

[http://community.whitehatsec.com/whitehat\\_arsenal.html](http://community.whitehatsec.com/whitehat_arsenal.html)

Platforms: FreeBSD, Linux, Windows 2000, Windows 95/98, Windows NT, Windows XP

Summary:

WHArsenal is designed to be the next generation of professional web security audit software. Architected from the ground up to be a generic web application security productivity tool, WHArsenal gives security professionals and web developer's access to the tools they need to make the job securing web applications faster and easier. WHArsenal possesses a powerful suite of GUI–Browser based web security tools. These endowments make WHArsenal capable of completing painstaking web security pen–test work considerably faster and more effectively than any of the currently available tools.

## VI. SPONSOR INFORMATION

---

This issue is sponsored by: FastTrain

FastTrain has your solution for a great CISSP Boot Camp. The industry's most recognized corporate security certification track, provides a comprehensive prospectus based upon the core principle concepts of security. This ALL INCLUSIVE curriculum utilizes lectures, case studies and true hands–on utilization of pertinent security tools. For a limited time you can enter for a chance to win one of the latest technological innovations, the SEGWAY HT.

Log onto <http://www.fasttraincamp.com>.

---

FastTrain has your solution for a great CISSP Boot Camp. The industry`s most recognized corporate security certification track, provides a comprehensive prospectus based upon the core principle concepts of security. This ALL INCLUSIVE curriculum utilizes lectures, case studies and true hands–on utilization of pertinent security tools. For a limited time you can enter for a chance to win one of the latest technological innovations, the SEGWAY HT. Log onto <http://www.fasttraincamp.com>.

---