

# SecurityFocus Microsoft Newsletter #153

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-09/0048.html>

---

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

**Date:** 09/08/03

Date: Mon, 8 Sep 2003 13:47:49 -0600 (MDT)

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

SecurityFocus Microsoft Newsletter #153

---

This Issue is Sponsored by BlackHat

Attend Black Hat Briefings & Training Federal, September 29–30 (Training), October 1–2 (Briefings) in Tysons Corner, VA; the world's premier technical IT security event. Modeled after the famous Black Hat event in Las Vegas! 6 tracks, 12 training sessions, top speakers and sponsors. Symantec is the Diamond sponsor. Early-bird registration ends September 6.

[http://www.securityfocus.com/sponsor/BlackHat\\_ms-secnews\\_030902](http://www.securityfocus.com/sponsor/BlackHat_ms-secnews_030902)

---

## I. FRONT AND CENTER

1. Intrusion Detection Terminology (Part One)

## II. MICROSOFT VULNERABILITY SUMMARY

1. File Sharing for Net Directory Traversal File Disclosure Vul...
2. ZoneAlarm Random UDP Flood Denial Of Service Vulnerability
3. Wrapsody View Copy And Paste Restriction Bypassing Vulnerabi...
4. FloosieTek FTGatePro Mail Server Path Disclosure Vulnerabili...
5. FloosieTek FTGatePro Mail Server Cross-Site Scripting Vulner...
6. Microsoft mshtml.dll Library GIF Image Handling Denial of Se...
7. Microsoft Windows XP TCP Packet Information Leakage Weakness
8. Microsoft Windows NetBIOS Name Service Reply Information Lea...
9. Microsoft Word Macro Execution Security Model Bypass Vulnera...
10. Microsoft Visual Basic For Applications Document Handling Bu...
11. Microsoft Access Snapshot Viewer ActiveX Control Parameter B...
12. Microsoft WordPerfect Converter Buffer Overrun Vulnerability
13. Ipswitch WS\_FTP Server FTP Command Buffer Overrun Vulnerabil...
14. Microsoft Windows 98 Fragmented UDP Flood Denial Of Service ...
15. Multiple Blackberry Enterprise Server Vulnerabilities

## III. MICROSOFT FOCUS LIST SUMMARY

1. Domain vs. Local security policy (Thread)
2. windows 2000 security logs (Thread)
3. Local Admins (Thread)

4. MS03-008 and SP4 (Thread)
5. focus-ms@securityfocus.com (Thread)
6. windows update (Thread)
7. Security Configuration guides provided by the Navy. (Thread)
8. cached passwords (was focus-ms@securityfocus.com) (Thread)

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Sophos Anti-Virus
2. LANDesk Management Suite 7
3. McAfee ePolicy Orchestrator
4. Enterprise Manager
5. ZoneAlarm Pro 4.0
6. ActiveScout Enterprise

#### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. The OpenAntivirus Project: Summary Various
2. BO2K v1.1.1
3. OSIRIS v2.0.0b
4. SysOrb v2.4.2
5. ccrypt v1.6
6. Star v1.5a21

#### VI. SPONSOR INFORMATION

##### I. FRONT AND CENTER

-----

###### 1. Intrusion Detection Terminology (Part One)

By Andy Cuff

This is the first of a two-part series that discusses IDS terminology, including terms where there may be disagreement from within the security community.

<http://www.securityfocus.com/infocus/1728>

##### II. MICROSOFT VULNERABILITY SUMMARY

-----

###### 1. File Sharing for Net Directory Traversal File Disclosure Vul...

BugTraq ID: 8513

Remote: Yes

Date Published: Aug 30 2003

Relevant URL: <http://www.securityfocus.com/bid/8513>

Summary:

File Sharing for Net is a web server program designed to share documents and files over the Web. It is available for the Microsoft Windows operating system.

File Sharing for Net is said to be prone to a directory traversal vulnerability, potentially allowing users to disclose the contents of system files. The problem occurs due to the application failing to parse user-supplied input for directory traversal sequences (../), thus making it possible to access files outside of the established web root.

This could potentially allow an attacker to obtain information that could be used in launching further attacks, such as passwords or sensitive user information.

This vulnerability is said to affect File Sharing for Net 1.5.

## 2. ZoneAlarm Random UDP Flood Denial Of Service Vulnerability

BugTraq ID: 8525

Remote: Yes

Date Published: Sep 02 2003

Relevant URL: <http://www.securityfocus.com/bid/8525>

Summary:

ZoneAlarm is a firewall software package available for the Microsoft Windows operating system. It is distributed and maintained by Zone Labs.

A denial of service vulnerability has been alleged in ZoneAlarm. It is reportedly possible to reproduce this condition by sending a flood of UDP packets to random ports (0–65000) on a system hosting the vulnerable software. This issue reportedly presents itself because ZoneAlarm takes longer to handle some packets than others.

It has been reported that this type of attack has the potential to cause vsmon to consume system resources, causing the remote affected system to behave in an unstable manner and suffer from performance degradation issues. Additionally it has been reported that outgoing UDP based services, for example ICQ client, may be denied. It has been reported that the UDP flood may have to be in the region of 900Kb of UDP based data a second to trigger this issue.

## 3. Wrapsody View Copy And Paste Restriction Bypassing Vulnerabi...

BugTraq ID: 8526

Remote: No

Date Published: Sep 02 2003

Relevant URL: <http://www.securityfocus.com/bid/8526>

Summary:

Wrapsody is a file and e-mail content security application distributed and maintained by Fasoo.com. It is available for the Microsoft Windows platform.

A problem has been discovered in the default workflow deployed with the Wrapsody viewer. Because of this, an attacker may be able to perform unauthorized actions on a vulnerable system.

The problem is in the implementation the workflow used by Wrapsody. By loading a specific workflow, an attacker may be able to circumvent restrictions placed on content, performing copy and paste actions.

## 4. FloosieTek FTGatePro Mail Server Path Disclosure Vulnerabili...

BugTraq ID: 8527

Remote: Yes

Date Published: Sep 02 2003

Relevant URL: <http://www.securityfocus.com/bid/8527>

Summary:

FloosieTek FTGatePro Mail Server is a mail server implementation for Microsoft Windows operating systems.

FloosieTek FTGatePro Mail Server may disclose its installation path to remote attackers. The issue reportedly occurs when '/utility/wmsecurity.fts' is requested by a remote user. This information could be useful in aiding the attacker to enumerate the layout of the file system on the host, which could result in further attacks against the host.

This issue exists in the web administrative interface, which listens on port 8089 by default.

#### 5. FloosieTek FTGatePro Mail Server Cross-Site Scripting Vulner...

BugTraq ID: 8528

Remote: Yes

Date Published: Sep 02 2003

Relevant URL: <http://www.securityfocus.com/bid/8528>

Summary:

FloosieTek FTGatePro Mail Server is a mail server implementation for Microsoft Windows operating systems.

FloosieTek FTGatePro Mail Server is prone to a cross-site scripting vulnerability. The source of this vulnerability is that HTML and script code supplied via URI parameters is not sufficiently filtered before being echoed back in web pages. In particular, it is possible to inject HTML and script code into the 'href' parameter of '/help/index.fts'.

A remote attacker could exploit this issue by enticing a legitimate user of the mail server to follow a malicious link with embedded HTML and script code. The attacker-supplied code would potentially be rendered in the user's browser when the link is followed.

This issue could potentially be exploited to steal cookie-based authentication credentials from a legitimate user. Other attacks are also possible.

This issue exists in the web administrative interface, which listens on port 8089 by default.

#### 6. Microsoft mshtml.dll Library GIF Image Handling Denial of Se...

BugTraq ID: 8530

Remote: Yes

Date Published: Sep 02 2003

Relevant URL: <http://www.securityfocus.com/bid/8530>

Summary:

An unidentified denial of service vulnerability has been discovered in the Microsoft mshtml.dll library. The problem is believed to occur when handling malformed GIF images, possibly with invalid header information.

Although unconfirmed, the image may be required to be 1x1 pixels to trigger this condition. Furthermore, for the denial of service to be triggered it is believed that the image must not be located in temporary internet files.

The denial of service may be triggered when an application linked to the library attempts to interpret an HTML document containing the malformed image, such as Internet Explorer or Microsoft Outlook.

It has been conjectured that the crash occurs due to the library attempting to dereference invalid memory, due to malformed data within the image file. However, this information has not been confirmed.

The precise technical details of this issue are currently unknown, however this BID will be updated as further information is made available.

#### 7. Microsoft Windows XP TCP Packet Information Leakage Weakness

BugTraq ID: 8531

Remote: Yes

Date Published: Sep 02 2003

Relevant URL: <http://www.securityfocus.com/bid/8531>

Summary:

A weakness has been discovered in Microsoft Windows XP. The problem occurs due to Windows XP failing to sufficiently initialize specific locations in memory, prior to using their values within TCP packets.

As a result of this issue, an attacker may be capable of viewing the contents of previously used system memory. This can be accomplished by intercepting SYN packets transmitted by an affected Microsoft Windows XP host, and observing the contents of the unused URG flag. This flag value may contain 16 bits of previously used system memory. By intercepting a sequence of these packets, it is theoretically possible for an attacker to obtain sensitive information previously contained within memory, such as a password. It should be noted that memory disclosed via this weakness will be random and will not be sensitive under most circumstances.

The precise technical details regarding this weakness are currently unknown. However, this BID will be updated as more information is made available.

#### 8. Microsoft Windows NetBIOS Name Service Reply Information Lea...

BugTraq ID: 8532

Remote: Yes

Date Published: Sep 03 2003

Relevant URL: <http://www.securityfocus.com/bid/8532>

Summary:

A weakness has been reported in NetBIOS on Microsoft Windows operating systems that may enable remote attackers to gain access to potentially sensitive information. In particular, the NetBIOS Name Service may leak random memory contents when replying to NetBT Name Service requests.

The source of this issue is a flaw in how NetBT pads datagrams. A larger buffer is allocated than is needed when NetBIOS is generating a Name Service reply and this buffer is not adequately initialized before the reply is generated. As a result, the reply may contain random fragments of system memory, some of which could potentially contain sensitive information. It is reported that the amount of padding that is required will normally be 15 bytes or less, which will cause minute amounts of memory to be disclosed, which will be derived from a previous memory operation. The expected behavior is for the datagram padding to be blank.

#### 9. Microsoft Word Macro Execution Security Model Bypass Vulnera...

BugTraq ID: 8533

Remote: Yes

Date Published: Sep 03 2003

Relevant URL: <http://www.securityfocus.com/bid/8533>

Summary:

Microsoft Word is a word processing software that is part of the Microsoft Office suite. Microsoft Word allows a user to create various types of documents. The software also supports the use of macros in order to automate commonly performed tasks.

Microsoft Word has been reported to be prone to a vulnerability that allows an attacker to bypass the macro security model of the software. The issue exists due to a failure in the software to ensure properties of a modified document with macros. This flaw allows the macro to be executed without prior notification to the user.

It has been reported that an attacker may exploit this issue by embedding malicious macro instructions within a document, which is crafted in a manner sufficient to trigger the vulnerability. When opened, the malicious macro contained within this document would be executed despite the macro security settings of Microsoft Word.

If successful, this attack would allow an attacker to execute arbitrary code within the context of the user who is running the affected software. The vulnerable system could be exploited in terms of data modifications, backdoor programs, and reformatting of the hard drives etc. An attack may also change the macro security setting of Microsoft Word, that could lead to execution of macros previously blocked by the user. If the user has administrative privileges, an attacker may completely compromise the system.

#### 10. Microsoft Visual Basic For Applications Document Handling Bu...

BugTraq ID: 8534

Remote: Yes

Date Published: Sep 03 2003

Relevant URL: <http://www.securityfocus.com/bid/8534>

Summary:

Microsoft Visual Basic for Applications (VBA) is a development platform implemented by various applications. A buffer overrun vulnerability has been discovered in VBA when handling malformed documents. The issue exists

in all applications that implement the use of VBA, such as Microsoft Office products.

The vulnerability occurs due to insufficient bounds checking when the application parses the contents of a document that supports VBA, such as a Word, Excel, or PowerPoint file. The issue exists in the Visual Basic Design Time Environment library and may be triggered by a malformed document property. As a result, if the malicious document is passed to the application, it may be possible to trigger the buffer overrun, triggering the corruption of memory adjacent to the originally assigned memory buffer.

Potentially, an attacker could exploit this issue to corrupt sensitive memory variables crucial to the execution flow of the affected application. Successful exploitation would effectively result in the execution of arbitrary code with the privileges of the affected application.

Internet Explorer is also reportedly an attack vector, since it may automatically call helper applications when handling certain document types.

This vulnerability affects Microsoft VBA 5.0 through 6.3, which ship with a number of other Microsoft products.

#### 11. Microsoft Access Snapshot Viewer ActiveX Control Parameter B...

BugTraq ID: 8536

Remote: Yes

Date Published: Sep 03 2003

Relevant URL: <http://www.securityfocus.com/bid/8536>

##### Summary:

Microsoft Access Snapshot Viewer, is a utility used to view a snapshot of a Microsoft Access database on systems that do not have Microsoft Access installed. The snapshot view is installed by default on all systems that have Microsoft Access installed; additionally the Microsoft Access Snapshot Viewer may be downloaded as an ActiveX control (Snapview.ocx).

Microsoft Access Snapshot Viewer has been reported prone to a remote buffer overflow condition. The vendor has reported that the issue presents itself, due to a lack of sufficient boundary checks performed on user-supplied parameters.

Although unconfirmed, it has been conjectured that by passing excessive data to the affected ActiveX control, the bounds of an insufficient reserved buffer in memory may be overrun and adjacent memory corrupted with attacker-supplied values. To exploit this issue, the vulnerable control may be called with malformed parameters by a malicious web page. It has been conjectured that an attacker may leverage this issue, to ultimately execute arbitrary instructions in the context of the user running the affected Internet Explorer.

It should be noted that although Microsoft Access 2002, 2000 and 97 are reported prone to this vulnerability. Previous versions may also be affected.

#### 12. Microsoft WordPerfect Converter Buffer Overrun Vulnerability

BugTraq ID: 8538

Remote: No

Date Published: Sep 03 2003

Relevant URL: <http://www.securityfocus.com/bid/8538>

Summary:

Microsoft WordPerfect Converter is a component shipped with Office and a number of other Microsoft products for handling documents in WordPerfect formats. The WordPerfect Converter is also available separately from Microsoft as part of the Office Converter Pack.

A buffer overrun vulnerability has been reported in the converter. The issue is due to insufficient bounds checking of parameters in WordPerfect documents. A particularly malformed WordPerfect document could potentially corrupt adjacent regions of process memory with attacker-supplied data. An attacker could leverage this condition to control execution flow and cause the execution of malicious instructions. This would occur in the context of the user opening the malformed document.

#### 13. Ipswitch WS\_FTP Server FTP Command Buffer Overrun Vulnerabil...

BugTraq ID: 8542

Remote: Yes

Date Published: Sep 04 2003

Relevant URL: <http://www.securityfocus.com/bid/8542>

Summary:

Ipswitch WS\_FTP Server is an FTP implementation that is available for Microsoft Windows operating systems.

Ipswitch WS\_FTP Server is reported to be prone to buffer overruns when handling data supplied to the APPE and STAT FTP commands. An FTP user who supplies excessive input to these commands could potentially execute arbitrary code in the context of the server or cause a denial of service.

The issues may be reproduced by supplying arguments to these commands that are in excess of 255 characters. This will cause adjacent regions of memory to be corrupted with the excessive data. By overwriting sensitive regions of memory, such as instruction pointers, it may be possible to exploit this issue to control execution flow of the server process. In this manner, it will be possible to execute arbitrary code in the context of the server, which may be run as SYSTEM.

A similar issue with the STAT command is described in BID 3507, but was addressed by the vendor in a previous release.

#### 14. Microsoft Windows 98 Fragmented UDP Flood Denial Of Service ...

BugTraq ID: 8543

Remote: Yes

Date Published: Sep 04 2003

Relevant URL: <http://www.securityfocus.com/bid/8543>

Summary:

A remote denial of service vulnerability has been reported to affect Microsoft Windows 98. It is reportedly possible to reproduce this condition by sending a fragmented flood of spoofed UDP packets to a vulnerable system. This will reportedly consume system resources and may ultimately result in the system locking up until the attack desists.

Ultimately exploitation of this issue will reportedly exhaust system resources, potentially denying availability of the operating system.

This vulnerability has been reported to affect Microsoft Windows 98, but not Windows 98SE. It should be noted that this issue might also affect prior Windows versions.

This is likely a known issue.

#### 15. Multiple Blackberry Enterprise Server Vulnerabilities

BugTraq ID: 8544

Remote: Yes

Date Published: Sep 04 2003

Relevant URL: <http://www.securityfocus.com/bid/8544>

Summary:

Blackberry Enterprise Server is communications middleware for Research In Motion Blackberry devices. It is distributed and maintained by Blackberry, and available for the Microsoft Windows platform.

Several issues have been identified in Blackberry Enterprise Server. Because of these issues, an attacker may be able to deny service to legitimate users of a host using the software, or gain unauthorized privileges.

The following problems are known:

Under some circumstances, a resource exhaustion vulnerability occurs when handling large or complex documents. This has been noted with PDF documents, and results in 100% CPU utilization for several minutes. Exploitation of this issue may be repeated to result in prolonged denial of service. This issue is resolved in release 3.6 Service Pack 1a.

A problem with password management occurs when the same document is sent to a user twice. A password-protected attachment sent to a user a second time may be viewed without entering a password if the document has been sent to the recipient and password entered previously. This issue likely occurs due to storage of password credentials in system memory. This issue is resolved in release 3.6 Service Pack 1a.

A problem with password management occurs when the same password-protected document is sent to multiple users. Upon one user entering the password

for the document, all recipients of the document may view the contents of the protected document. This issue is resolved in release 3.6 Service Pack 1a.

Some configurations with the Cache Size value set to 32 could experience resource consumption, resulting in a temporary denial of service. This occurs when the table of contents of a large file is retrieved. An attacker could continuously perform this action to cause an extended denial of service. This issue is resolved in release 3.6 Service Pack 1a.

The extended logging level of the Blackberry Enterprise Server software does not correctly display extended data. This configuration could result in the unintended loss of sensitive information. This issue is resolved in release 3.6 Service Pack 1a.

Blackberry Enterprise Server does not adequately protect the SQL user credentials when storing them. The software stores SQL user passwords in the registry in plain text. An attacker with read access to the system registry may gain access to the database. This issue exists in 3.6 Service Pack 1a.

In some configurations, sending the Set Password and Lock IT command sent via the administrative console does not lock the device as intended. Due to handling of passwords by the software, the device may lock without adequate security measures, allowing the user of the target device to unlock the device by double-clicking. This issue exists in 3.6 Service Pack 1a.

This BID will be divided into individual BIDs when further analysis of the issues is complete.

### III. MICROSOFT FOCUS LIST SUMMARY

---

1. Domain vs. Local security policy (Thread)  
Relevant URL:

<http://www.securityfocus.com/archive/88/336532>

2. windows 2000 security logs (Thread)  
Relevant URL:

<http://www.securityfocus.com/archive/88/336531>

3. Local Admins (Thread)  
Relevant URL:

<http://www.securityfocus.com/archive/88/336479>

4. MS03-008 and SP4 (Thread)  
Relevant URL:

<http://www.securityfocus.com/archive/88/336477>

5. focus–ms@securityfocus.com (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/336476>

6. windows update (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/336311>

7. Security Configuration guides provided by the Navy. (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/336246>

8. cached passwords (was focus–ms@securityfocus.com) (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/335812>

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

-----

##### 1. Sophos Anti–Virus

By: Sophos

Platforms: AIX, DOS, FreeBSD, HP–UX, Linux, MacOS, Netware, OS/2, Solaris, UNIX, VMS, Windows 3.x, Windows 95/98, Windows NT

Relevant URL: <http://www.sophos.com/products/sav/>

Summary:

Sophos Anti–Virus is a unique solution to the virus problem, providing true cross–platform protection in a single, fully integrated product. The network–centric design provides a host of benefits for the protection of servers, workstations and portables. Sophos's ground–breaking architecture maximises protection, while minimising performance and administrative overheads.

##### 2. LANDesk Management Suite 7

By: LANDesk Software

Platforms: AIX, HP–UX, Linux, MacOS, Solaris, Windows 2000, Windows 95/98, Windows NT, Windows XP

Relevant URL: <http://www.landesk.com/products/ilms/>

Summary:

LANDesk Management Suite 7 is a comprehensive, integrated management solution that's easy to use. Enabling proactive management of desktops, server and mobile devices across heterogeneous IT environments.

- Keep up with security patches and virus updates
- Efficiently install and maintain software on the desktop
- Decrease software license costs and respond to audits

- Reduce the cost of helpdesk support
- Discover and manage hardware and software assets
- Migrate many users and their profiles to new operating systems

### 3. McAfee ePolicy Orchestrator

By: Network Associates

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

Relevant URL:

<http://www.nai.com/us/products/mcafee/antivirus/fileserver/epo.htm>

Summary:

McAfee Security ePolicy Orchestrator (ePO) is the market-leading tool for centralized policy management of malicious threat protection. ePO allows you to maintain up-to-date protection, configure and enforce policies, and generate detailed graphical reports on McAfee Security and third party products, including Symantec and Dr Ahn anti-virus products.

### 4. Enterprise Manager

By: Sophos

Platforms: Windows 2000, Windows NT

Relevant URL: <http://www.sophos.com/products/em/>

Summary:

The Enterprise Manager suite is a powerful set of tools allowing fully automated web-based installation and updating of Sophos software across a network and even to remote users.

Network administrators are put in full control and can monitor their network at all times. Unprotected computers or those running an out-of-date version of Sophos Anti-Virus can be immediately and automatically updated. In practice, a network of 1000 or more clients can be updated from a single, central Windows machine within five minutes.

### 5. ZoneAlarm Pro 4.0

By: Zone Labs

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

Relevant URL: <http://www.zonelabs.com>

Summary:

Hackers lurk everywhere on the Internet, waiting for an "in" into your personal and financial information. Even legitimate Web sites have sophisticated methods of snooping, such as cookies that track your identity and browsing habits. You need nothing less than the industry's best protection?ZoneAlarm Pro. It offers you the award-winning firewall that Zone Labs is famous for. Plus, it stops annoying and potentially malicious cookies and pop-ups from invading your system.

### 6. ActiveScout Enterprise

By: ForeScout Technologies

Platforms: Linux, Solaris, Windows 2000, Windows 95/98, Windows NT

Relevant URL: <http://www.forescout.com/enterprise.html>

Summary:

ActiveScout Enterprises actively protects a network with multiple access points. In addition to the identification of attackers and automatic action to stop them, this solution offers full management capabilities, from configuration and reporting, to the sharing of threat information between multiple deployed scouts.

## V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

### 1. The OpenAntivirus Project: Summary Various

By: cbricart, fz-net, hfuhs, kurti and reniar

Relevant URL: <http://www.openantivirus.org/>

Platforms: Os Independent, POSIX, Windows 2000, Windows 95/98, Windows NT, Windows XP

Summary:

Developing Open Source AntiVirus Solutions

### 2. BO2K v1.1.1

By: andrereis and j\_aroche

Relevant URL: <http://www.bo2k.com/>

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

Summary:

BO2K is a remote administration tool for Windows systems. It comes with a client and a server. The server is lightweight and inobtrusive. A dynamic plugin architecture allows for easy system extension.

### 3. OSIRIS v2.0.0b

By: The Shmoo Group

Relevant URL: <http://osiris.shmoo.com>

Platforms: BSDI, FreeBSD, Linux, MacOS, OpenBSD, UNIX, Windows 2000, Windows NT, Windows XP

Summary:

Osiris is a host integrity management system that can be used to monitor changes to a network of hosts over time and report those changes back to the administrator(s). Currently, this includes monitoring any changes to the filesystems. Osiris takes periodic snapshots of the filesystem and stores them in a database. These databases, as well as the configurations and logs, are all stored on a central management host. When changes are detected, Osiris will log these events to the system log and optionally send email to an administrator. In addition to files, Osiris has preliminary support for the monitoring of other system information including user lists, file system details, kernel modules, and network interface configurations (not included with in this beta release).

### 4. SysOrb v2.4.2

By: oestergaard

Relevant URL: <http://www.sysorb.com/>

Platforms: FreeBSD, Linux, Solaris, SunOS, Windows 2000, Windows NT

Summary:

SysOrb is a client/server package that can monitor servers remotely (such as Web servers), or monitor devices on servers (such as disks, memory, load, etc.). It will alert the administrators via e-mail or pager if a server is entering a critical condition, and has its own database backend, allowing for massive collection of system statistics.

5. ccrypt v1.6

By: Peter Selinger

Relevant URL: <http://quasar.mathstat.uottawa.ca/~selinger/ccrypt/>

Platforms: AIX, FreeBSD, Linux, MacOS, Solaris, SunOS, Windows 2000, Windows 95/98, Windows NT

Summary:

ccrypt is a commandline utility for encrypting and decrypting files and streams. It was designed as a replacement for the standard Unix crypt utility, which is notorious for using a very weak encryption algorithm. ccrypt is based on the Rijndael cipher, which is the U.S. government's chosen candidate for the Advanced Encryption Standard (AES). This cipher is believed to provide very strong security. A compatibility mode is included for decrypting legacy "unix crypt" files.

6. Star v1.5a21

By: Jörg Schilling

Relevant URL:

<http://www.fokus.gmd.de/research/cc/gclone/employees/joerg.schilling/private/star.html>

Platforms: BeOS, MacOS, OS/2, POSIX, Windows 2000, Windows 95/98, Windows NT, Windows XP

Summary:

Star is a very fast, POSIX-compliant tar archiver. It reads and writes POSIX compliant tar archives as well as non-POSIX GNU tar archives. Star is the first free POSIX.1-2001 compliant tar implementation. It saves many files together into a single tape or disk archive, and can restore individual files from the archive. It includes a FIFO for speed, a pattern matcher, multi-volume support, the ability to archive sparse files and ACLs, the ability to archive extended file flags, automatic archive format detection, automatic byte order recognition, automatic archive compression/decompression, remote archives, and special features that allow star to be used for full and incremental backups. It includes the only known platform independent "rmt" server program that hides Linux incompatibilities. The "rmt" server from the star package implements all Sun/GNU/Schily/BSD enhancements and allows any "rmt" client from any OS to contact any OS as server.

## VI. SPONSOR INFORMATION

-----  
This Issue is Sponsored by BlackHat

## SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #153

Attend Black Hat Briefings & Training Federal, September 29–30 (Training), October 1–2 (Briefings) in Tysons Corner, VA; the world's premier technical IT security event. Modeled after the famous Black Hat event in Las Vegas! 6 tracks, 12 training sessions, top speakers and sponsors. Symantec is the Diamond sponsor. Early–bird registration ends September 6.

[http://www.securityfocus.com/sponsor/BlackHat\\_ms-secnews\\_030902](http://www.securityfocus.com/sponsor/BlackHat_ms-secnews_030902)

---

KaVaDo provides the first and only integrated Web application scanner and firewall security suite that prevent Web applications attacks, the most common form of online exploitation. Download a FREE whitepaper on Security Policy Automation for Web Applications.

[http://www.securityfocus.com/sponsor/KaVaDo\\_focus-ms\\_030818](http://www.securityfocus.com/sponsor/KaVaDo_focus-ms_030818)

---