

# SecurityFocus Microsoft Newsletter #145

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-07/0059.html>

---

**From:** Marc Fossi (*mfossi\_at\_securityfocus.com*)

**Date:** 07/14/03

Date: Mon, 14 Jul 2003 13:34:27 -0600 (MDT)

To: Focus-MS <focus-ms@securityfocus.com>

SecurityFocus Microsoft Newsletter #145

---

This Issue is Sponsored by: KaVoDo

Your network Firewall and IDS products do not prevent Web application exploits – the most common form of online attack – resulting in Web defacement, data theft, sabotage and fraud.

KaVaDo is the first and only company that provides a complete and an integrated suite of Web application security products, allowing you to assess your entire environment, automatically set positive security policies and maintain it without compromising business performance.

For more information on KaVaDo and to download a FREE white paper on Web applications – security policy automation, please visit <http://www.securityfocus.com/Kavado-ms-secnews2>

---

## I. FRONT AND CENTER

1. Linux Firewall-related /proc Entries
2. The Persistence of Hoax
3. U.S. Information Security Law, Part Four
4. The SecurityFocus 4th Anniversary Contest

## II. MICROSOFT VULNERABILITY SUMMARY

1. Mirabilis ICQ Password Bypass Weakness
2. Mini-Webserver Information Disclosure Vulnerability
3. Novell eDirectory DS/iMONITOR Unspecified Vulnerabilities
4. Microsoft URLScan Tool Information Disclosure Vulnerability
5. BillingExplorer Multiple Remote Client Communication Integrity...
6. Tower Toppler HOME Environment Variable Local Buffer Overflow...
7. Microsoft Windows 2000 ShellExecute() Buffer Overflow...
8. Microsoft Outlook Web Access HTML Attachment Script Execution...
9. IglooFTP PRO Multiple Buffer Overflow Vulnerabilities
10. Cerulean Studios Trillian Client Malformed TypingUser Denial...
11. Macromedia ColdFusion MX Remote Development Service File...

12. Macromedia ColdFusion MX Remote Development Service Default...
13. Microsoft RunDLL32.EXE Buffer Overflow Vulnerability
14. NetScreen Non-IP Traffic Firewall Bypass Vulnerability
15. MyServer Malformed URI Denial Of Service Vulnerability
16. Apache Web Server Type-Map Recursive Loop Denial Of Service...
17. UnrealIRCd OperServ Raw Join Denial Of Service Vulnerability
18. Apache Web Server FTP Proxy IPV6 Denial Of Service Vulnerability
19. Macromedia Apache Web Server Encoded Space Source Disclosure...
20. Apache Web Server Prefork MPM Denial Of Service Vulnerability
21. Microsoft Windows CreateFile API Named Pipe Privilege...

### III. MICROSOFT FOCUS LIST SUMMARY

1. How to generate list of patches installed? (Thread)
2. FW: Keyboard Locking/Invisible Screensaver (Thread)
3. Keyboard Locking/Invisible Screensaver (Thread)
4. investigating misuse of the internet (Thread)
5. Article Announcement: Antivirus Concerns in XP and .NET...
6. Administrivia: MS Spam Thread (Thread)
7. Article Announcement: Can Microsoft End Spam? (Thread)
8. SecurityFocus Microsoft Newsletter #144 (Thread)
9. How to block users from installing other apps (Thread)
10. Article Announcement: Penetration Testing for Web Applications...
11. Administrivia: Week of July 7, 2003 (Thread)
12. SP4 Installation Failure (Thread)

### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. AbsoluteEncrypt
2. Invisible Secrets 2002
3. ZDelete

### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Ettercap v0.6b
2. Anti-Spam SMTP Proxy v0.3.0
3. ScanADS - Scan Alternate Data Streams v1.1

### VI. SPONSOR INFORMATION

#### I. FRONT AND CENTER

---

1. Linux Firewall-related /proc Entries  
By Brian Hatch

This article will discuss Linux kernel variables and the effect they have on network security for your host or firewall. These variables determine the handling of network packets and are independent of any kernel filtering rules.

<http://www.securityfocus.com/infocus/1711>

2. The Persistence of Hoax  
By George Smith

Vmyths.com is fading into the sunset, while the virus hoaxes it steadfastly debunked seem to live on forever.

<http://www.securityfocus.com/columnists/172>

### 3. U.S. Information Security Law, Part Four By Steven Robinson

This is the last article in a four-part series looking at U.S. information security laws and the way those laws affect the work of security professionals. This installment continues the discussion of information security in the public sector and provides an overview of national security law in the United States as it pertains to information security.

<http://www.securityfocus.com/infocus/1710>

### 4. The SecurityFocus 4th Anniversary Contest

Only three days left to win a pair of passes to the Black Hat Briefings. Be sure to take a few minutes out of your day to enter the contest.

Please visit the contest page here:

<http://www.securityfocus.com/contest>

## II. BUGTRAQ SUMMARY

### 1. Mirabilis ICQ Password Bypass Weakness

BugTraq ID: 8111

Remote: No

Date Published: Jul 05 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8111>

Summary:

Mirabilis ICQ is an instant messenger client for a number of platforms including Microsoft Windows, MacOS and Palm systems.

An issue has been reported for ICQ that may result in an attacker obtaining access to another ICQ user's account.

The issue exists because the ICQ contact window, which is specific to a single user, may be accessed using the EnableWindow API. Through the use of this API, it is possible to access the victim user's ICQ account regardless of existing security measures.

Exploitation of this issue may result in a local user being able to access another local user's ICQ contact information.

### 2. Mini-Webserver Information Disclosure Vulnerability

BugTraq ID: 8122

Remote: Yes

Date Published: Jul 07 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8122>

Summary:

Mini-Webserver is a free web server implementation. It is available for Microsoft Windows operating systems.

It has been alleged that Mini-Webserver fails to adequately protect the contents of some directories installed by the server, such as 'Auth' and 'security'. It is possible for remote users to request files from these directories. This could expose sensitive information stored in these directories to remote attackers.

This issue could be related to web server configuration.

### 3. Novell eDirectory DS/iMONITOR Unspecified Vulnerabilities

BugTraq ID: 8141

Remote: Unknown

Date Published: Jul 08 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8141>

Summary:

eDirectory is a directory server software package distributed by Novell for the Microsoft Windows platform.

Novell has released eDirectory 8.6.2 SP4 for NetWare and NT Platforms. This service pack contains fixes to address a potential unspecified security issue in iMONITOR and also adds security enhancements to the Bindery supervisor in the DS.NLM module.

It is not currently clear whether these vulnerabilities are local or remote issues.

Further technical details are not available at the time of writing. This BID will be updated appropriately when additional technical information becomes available. Separate BIDs may be created for each individual issue where appropriate.

### 4. Microsoft URLScan Tool Information Disclosure Vulnerability

BugTraq ID: 8101

Remote: Yes

Date Published: Jul 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8101>

Summary:

Microsoft URLScan is a utility that is designed to restrict the types of HTTP requests that an IIS server will process.

Microsoft URLScan has been reported prone to an information disclosure vulnerability in some server configurations.

It has been reported that a remote attacker may disclose accurate IIS server HTTP header information, regardless of whether the server is protected by the URLScan tool 'RemoveServerHeader' functionality or not. The issue appears to present itself when an attacker makes a HTTPS request to an IIS server that is HTTPS enabled and protected by the Microsoft URLScan tool. A partial header may be returned to the attacker containing potentially sensitive version information. This issue may be as a result of conflicting configurations.

An attacker may use the information gathered in this way to aid in further attacks launched against the system.

It should be noted that an administrator who is implementing the URLScan tool might be lulled into a false sense of security by this issue.

While this vulnerability has been reported to affect Microsoft URLScan version 2.5, other versions might also be affected.

#### 5. BillingExplorer Multiple Remote Client Communication Integrity Vulnerabilities

BugTraq ID: 8123

Remote: Yes

Date Published: Jul 07 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8123>

Summary:

BillingExplorer is a commercially-available billing software package. It is available for the Microsoft Windows platform.

It has been reported that BillingExplorer does not properly handle some types of requests. Because of this, it is possible for a remote attacker to violate the integrity of billing and client communication.

The following issues have been identified:

It is possible to deny service to a legitimate client without knowing the login information for the target client. This can be by way of shutting down, restarting, or logging of the vulnerable client.

It is also possible to violate the integrity of billing information by sending a maliciously crafted request to the server. One can reset the timing tracked by the billing server to alter the total time charged by the server.

Other similar issues may also exist.

#### 6. Tower Toppler HOME Environment Variable Local Buffer Overflow Vulnerability

BugTraq ID: 8132

Remote: No

Date Published: Jul 08 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8132>

Summary:

Tower Toppler is a freely available, open source game for Linux and Microsoft operating systems.

A problem with the software may make elevation of privileges possible.

It has been reported that a buffer overflow exists in Tower Toppler. A local user may be able to exploit this issue to execute code with the privileges of the toppler program.

In some configurations, Toppler may be installed with setgid games privileges. Exploitation of this vulnerability could give the attacker group privileges of games.

#### 7. Microsoft Windows 2000 ShellExecute() Buffer Overflow Vulnerability

BugTraq ID: 8090

Remote: No

Date Published: Jul 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8090>

Summary:

The Windows 2000 ShellExecute() function is contained in the shell32.dll library. It can be used to launch applications such as a web browser.

The ShellExecute() function is prone to a boundary condition error. If an unusually large string is passed to the third parameter (lpszFile) of the function, an internal buffer will be overrun. This may result in a denial of service or potential arbitrary code execution.

This issue was reportedly fixed in Windows 2000 Service Pack 4, however, the vendor has not confirmed this.

#### 8. Microsoft Outlook Web Access HTML Attachment Script Execution Vulnerability

BugTraq ID: 8113

Remote: Yes

Date Published: Jul 05 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8113>

Summary:

Microsoft Outlook Web Access (OWA) is a component of Microsoft Exchange Server, used to provide a web interface for email.

OWA is web-based and supports HTML e-mail and HTML message attachments. OWA contains a vulnerability that may result in attacker-supplied script code executing within the context of the mail interface when processing e-mail containing HTML message attachments.

In a scenario where HTML message attachments are processed, it is possible to prevent filtering of the attachment. This can be achieved by ensuring that the generated URL, to view an attachment, does not contain the 'Security' URI parameter.

If did parameter does not exist, no filtering will be performed. Unfiltered, the script code will execute if embedded in an HTML email opened by a user.

The script code that executes may perform OWA actions as the user, such as sending or deleting email.

#### 9. IglooFTP PRO Multiple Buffer Overflow Vulnerabilities

BugTraq ID: 8117

Remote: Yes

Date Published: Jul 07 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8117>

Summary:

IglooFTP PRO is an FTP client that is designed for Linux and Microsoft Windows platforms.

IglooFTP PRO for Windows platforms has been reported prone to multiple buffer overrun vulnerabilities.

The issue likely presents itself due do a lack of sufficient bounds checking performed on data that is later copied into a reserved internal memory buffer. If an attacker supplies excessive data ( $\geq 1028$  bytes) in a manner sufficient to trigger the condition, data greater than the size of the assigned buffer may corrupt adjacent memory. Because adjacent memory has been reported to contain a saved instruction pointer, it is possible for an attacker to influence the execution flow of the vulnerable FTP client and execute arbitrary instructions.

Remote arbitrary code execution has been confirmed.

It should be noted that although this vulnerability has been reported to affect IglooFTP PRO version 3.8 for Windows platforms, other versions might also be affected.

#### 10. Cerulean Studios Trillian Client Malformed TypingUser Denial Of Service Vulnerability

BugTraq ID: 8107

Remote: Yes

Date Published: Jul 04 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8107>

Summary:

Trillian is an instant messaging client that supports a number of protocols (including IRC, ICQ, MSN). It is available for Microsoft Windows

systems.

Cerulean Studios Trillian client has been reported prone to a remotely exploitable denial of service vulnerability.

It has been reported that when a vulnerable client receives a malformed 'TypingUser' message, an internal exception will be triggered in the Trillian client and the client will likely fail. The issue has been reported to exist in a function within the msn.dll dynamic linked library.

It should be noted that although this issue has been reported to affect both Trillian 1 and 0.74, other versions might also be affected.

#### 11. Macromedia ColdFusion MX Remote Development Service File Disclosure Vulnerability BugTraq ID: 8109

Remote: Yes

Date Published: Jul 05 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8109>

Summary:

ColdFusion MX is the application server for developing and hosting infrastructure distributed by Macromedia. It is available as a standalone product for Unix, Linux, and Microsoft Operating Systems.

Remote Development Service (RDS) is a way to facilitate secure remote access to ColdFusion MX servers. This service is used by developers to access databases, files and other data sources. By default, the RDS service has SYSTEM level privileges.

A vulnerability has been reported for the RDS service that may allow an attacker to obtain unauthorized access to a data residing on a ColdFusion MX server. The vulnerability is due to the way that authentication is done when communicating with a ColdFusion MX server.

Specifically, RDS requires a password to authenticate a remote developer. However, it is possible for a remote user to configure their web site properties to access files residing on the vulnerable server.

Any information obtained in this manner may be used by an attacker to launch further attacks against a vulnerable system.

#### 12. Macromedia ColdFusion MX Remote Development Service Default Null Password Vulnerability BugTraq ID: 8110

Remote: Yes

Date Published: Jul 05 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8110>

Summary:

ColdFusion MX is the application server for developing and hosting infrastructure distributed by Macromedia. It is available as a standalone product for Unix, Linux, and Microsoft Operating Systems.

Remote Development Service (RDS) is a way to facilitate secure remote access to ColdFusion MX servers. This service is used by developers to access databases, files and other data sources. By default, the RDS service has SYSTEM level privileges.

It has been reported that, by default, the RDS service uses a blank password for authentication.

This could allow an unauthenticated user to access the vulnerable ColdFusion MX server.

### 13. Microsoft RunDLL32.EXE Buffer Overflow Vulnerability

BugTraq ID: 8114

Remote: No

Date Published: Jul 06 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8114>

Summary:

rundll32.exe is an application, shipped with Microsoft Windows, that is used to execute DLLs as programs; it is also used by many programs to execute functions/methods located in a DLL file.

rundll32.exe has been reported prone to a buffer overflow vulnerability. The condition has been reported to be triggered when an excessive string is passed to the vulnerable application as a routine name for a module.

The issue likely presents itself due do a lack of sufficient bounds checking performed on user-supplied routine name data that is copied into a reserved internal memory buffer. If a malicious user supplies excessive data (>499 bytes) in a manner sufficient to trigger the condition, data greater than the size of the assigned buffer may corrupt adjacent memory. Because adjacent memory has been reported to contain a saved instruction pointer, it is possible for an attacker to influence the execution flow of the vulnerable application and possibly execute arbitrary instructions.

Exploitation of this issue may be hindered, due to the fact that user-supplied data is converted to Unicode.

It should be noted that although this issue has been reported to affect the version of rundll32.exe that is shipped with Windows XP SP1, other versions might also be affected.

This issue has also been reported to affect Windows 2000 systems with service pack 4 installed, under certain circumstances. Specifically if the excessive data passed to the vulnerable application consists of '%' percentage characters, an attacker may corrupt the instruction pointer for

the affected process. Although unconfirmed it has been conjectured that this behaviour may be due to unicode formatting.

#### 14. NetScreen Non-IP Traffic Firewall Bypass Vulnerability

BugTraq ID: 8150

Remote: Yes

Date Published: Jul 09 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8150>

Summary:

NetScreen is a line of Internet security appliances integrating firewall, VPN and traffic management features. ScreenOS is the software used to manage and configure the firewall. NetScreen supports Microsoft Windows 95, 98, ME, NT and 2000 clients.

It has been alleged that it is possible for remote users to bypass NetScreen firewalls. Reports have stated that any non-IP or ARP traffic will bypass the firewall without being logged. Various protocols, such as SNA, IPX CDP, CDP, and VST may pass through the firewall unnoticed and without being filtered. This could permit an attacker to interact with hosts behind the firewall that support these various protocols.

This is reported to occur in 20x and 50x models when run in bridge mode, though this is not conclusive. This alleged vulnerability has not been confirmed by Symantec.

#### 15. MyServer Malformed URI Denial Of Service Vulnerability

BugTraq ID: 8120

Remote: Yes

Date Published: Jul 07 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8120>

Summary:

MyServer is a web server implementation for a number of platforms, including Microsoft Windows operating systems and Linux.

MyServer has been reported to be prone to denial of service attacks when handling certain malformed URIs. This issue may be due to a flaw in the CGI parser, causing the server to crash when some invalid CGI parameters are supplied. This could be exploited to deny availability of web services to legitimate users.

This issue was reported in myServer 0.4.2 on Microsoft Windows platforms. Other versions may also be affected.

#### 16. Apache Web Server Type-Map Recursive Loop Denial Of Service Vulnerability

BugTraq ID: 8138

Remote: No

Date Published: Jul 08 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8138>

Summary:

Apache is a freely available web server. It is available for a variety of platforms including the Unix, Linux and Microsoft Windows operating systems.

Apache content negotiation functionality reported prone to a denial of service vulnerability.

The issue may present itself, if an attacker has the ability to create a malicious type-map file. The attacker may craft the type-map file in a manner sufficient to cause the vulnerable server to fall into an infinite loop. It has been reported that the Apache server will exponentially consume resources in such circumstance. Effectively denying service to other legitimate system users.

#### 17. UnrealIRCd OperServ Raw Join Denial Of Service Vulnerability

BugTraq ID: 8131

Remote: Yes

Date Published: Jul 08 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8131>

Summary:

UnrealIRCd is an IRC implementation that is available for a number of platforms including Linux/Unix variants and Microsoft Windows operating systems.

It is reported UnrealIRCd may crash under some circumstances when a client sends a raw message tooperserv. This may occur when a raw message is used when requesting to join a channel. This will allegedly cause the server to segfault, resulting in a potential denial of service. It is not known if this condition could be exploited to corrupt memory and execute arbitrary code.

It should be noted that other IRC daemon implementations may be similarly affected, especially in cases where raw message code is shared with other implementations or derived from the same source.

The vulnerability is reported to exist in the `m_join()` function, which is included in the 's\_user.c' source file. It should be noted that other IRC daemon implementations may be similarly affected, especially in cases where raw message code is shared with other implementations or derived from the same source.

This issue is similar to BID 8130 but is being assigned a separate BID because it does seem like Anope Services is sharing the same vulnerable code with UnrealIRCd.

18. Apache Web Server FTP Proxy IPV6 Denial Of Service Vulnerability

BugTraq ID: 8135

Remote: Yes

Date Published: Jul 08 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8135>

Summary:

Apache is a freely available web server. It is available for a variety of platforms including the Unix, Linux and Microsoft Windows operating systems.

A denial of service vulnerability has been reported by the vendor to affect the FTP proxy component of Apache. It has been reported that an attacker may specify a target server that possesses an IPV6 address. This may result in a denial of service to other legitimate users. The issue reportedly presents itself, because the proxy server fails to create an IPV6 socket.

Explicit technical details regarding this vulnerability are not currently known, this BID will be updated as further details are disclosed.

19. Macromedia Apache Web Server Encoded Space Source Disclosure Vulnerability

BugTraq ID: 8136

Remote: Yes

Date Published: Jul 08 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8136>

Summary:

ColdFusion and JRun are web application delivery software packages available for the Unix, Linux, and Microsoft Windows platform.

It has been reported that an issue exists in Macromedia ColdFusion and JRun that could allow an attacker to gain unauthorized access to potentially sensitive information. This may result in an attacker gaining access to system resources.

The problem is in the disclosure of sensitive information contained in ColdFusion and Java Servlet Pages. By placing a request ending in an encoded space to the Apache Web Server packaged with ColdFusion MX and/or JRun, it is possible for the attacker to view the source of the web scripts hosted on the system.

It should be noted that this problem affects ColdFusion and JRun only on the Microsoft Windows platforms.

20. Apache Web Server Prefork MPM Denial Of Service Vulnerability

BugTraq ID: 8137

Remote: Yes

Date Published: Jul 08 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8137>

Summary:

Apache is a freely available web server. It is available for a variety of platforms including the Unix, Linux and Microsoft Windows operating systems.

Apache may be run as a non-threaded, pre-forking server via the prefork MPM (Multi-Processing Module).

The Apache Software Foundation has reported a vulnerability in the prefork MPM that could result in a temporary denial of service condition. This condition is known to occur when an accept() call on a rarely accessed port returns certain errors.

Further technical details are not available at the time of writing. This BID will be updated appropriately when additional technical information becomes available.

#### 21. Microsoft Windows CreateFile API Named Pipe Privilege Escalation Vulnerability

BugTraq ID: 8128

Remote: No

Date Published: Jul 08 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8128>

Summary:

A problem in Microsoft Windows 2000 may make it possible for a local user to gain elevated privileges.

It has been reported that Microsoft Windows does not properly handle named pipes. Because of this, an attacker may be able to gain access to the SYSTEM account.

The problem is in the access control mechanism of CreateFile API. There is no means of limiting what types of files are manipulated through the CreateFile call, allowing one to exploit this call to potentially perform nefarious activities.

Problems with the implementation of named pipes are a well-known issue in Microsoft Windows, and papers currently exist detailing the problems. Also, this problem may be the root of the issue of other known vulnerabilities in Microsoft Windows packages. Bugtraq IDs 3185 and 8098 are examples of other problems in named pipes which may be related, though there is no currently no information available confirming this.

### III. MICROSOFT FOCUS LIST SUMMARY

#### 1. How to generate list of patches installed? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/328722>

2. FW: Keyboard Locking/Invisible Screensaver (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/328723>

3. Keyboard Locking/Invisible Screensaver (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/328616>

4. investigating misuse of the internet (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/328618>

5. Article Announcement: Antivirus Concerns in XP and .NET Environments (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/328492>

6. Administrivia: MS Spam Thread (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/328502>

7. Article Announcement: Can Microsoft End Spam? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/328438>

8. SecurityFocus Microsoft Newsletter #144 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/328278>

9. How to block users from installing other apps (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/328272>

10. Article Announcement: Penetration Testing for Web Applications (Part Two) (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/328019>

11. Administrivia: Week of July 7, 2003 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/327908>

12. SP4 Installation Failure (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/327907>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

---

1. AbsoluteEncrypt

by Absolute Software

<http://www.absolute.com/public/products/absoluteencrypt/default.asp>

Platforms: Windows 2000, Windows XP

Summary:

Delivered as a software service or as enterprise software, AbsoluteEncrypt is a centrally managed desktop security solution that ensures the intellectual property, employee information and confidential data stored on your remote, mobile and desktop PCs is secure. A key component of an overall security strategy, AbsoluteEncrypt encrypts sensitive information on employees' desktops and prevents unauthorized access to private files. vWith AbsoluteEncrypt, organizations can proactively enforce data security policies while enhancing user productivity and avoiding extensive setup and ongoing administrative costs. Real time alerts help administrators address non-compliance immediately to protect against data security breaches and the cost of data falling into the wrong hands.

2. Invisible Secrets 2002

by Neobyte Solutions

<http://www.neobytesolutions.com/invsecr/index.html>

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

Summary:

Invisible Secrets 2002 not only encrypts your data and files for safe keeping or for secure transfer across the net, it also hides them in places that on the surface appear totally innocent, such as picture or sound files, or web pages. These types of files are a perfect disguise for sensitive information. Nobody, not even your wife, boss, or a hacker would realize that your important papers or letters are stored in your last holiday pictures, or that you use your personal web page to exchange messages or secret documents. With Invisible Secrets 2002 you may encrypt and hide files directly from Windows Explorer, and then automatically transfer them by e-mail or via the Internet. Invisible Secrets 2002 features strong encryption algorithms, a wizard that guides you through all the necessary steps needed to protect your data, a password management solution that stores all your passwords securely and helps you create secure passwords and a shredder that helps you destroy the originals after encryption.

3. ZDelete

by LSoft Technologies Inc.

<http://www.zdelete.com/>

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

Summary:

ZDelete is designed to permanently erase computer files, temporary Internet files, cookies, Internet history, and recently used files and documents. An integrated disk wiper included can also clear out all available/free disk space. It makes the recovery of files previously removed from the drive impossible.

## V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

### 1. Ettercap v0.6b

by ALoR alor@users.sourceforge.net

Relevant URL:

<http://ettercap.sourceforge.net/>

Platforms: FreeBSD, Linux, MacOS, NetBSD, Windows 2000, Windows NT, Windows XP

Summary:

Ettercap is a network sniffer/interceptor/logger for ethernet LANs. It supports active and passive dissection of many protocols (even ciphered ones, like SSH and HTTPS). Data injection in an established connection and filtering on the fly is also possible, keeping the connection synchronized. Many sniffing modes were implemented to give you a powerful and complete sniffing suite. Plugins are supported. It has the ability to check whether you are in a switched LAN or not, and to use OS fingerprints (active or passive) to let you know the geometry of the LAN.

### 2. Anti-Spam SMTP Proxy v0.3.0

by John Hanna

Relevant URL:

<http://assp.sourceforge.net/>

Platforms: Linux, MacOS, Os Independent, POSIX, UNIX, Windows 2000, Windows NT

Summary:

The Anti-Spam SMTP Proxy (ASSP) Server project aims to create an open source platform independent SMTP Proxy server which implements whitelists and Bayesian filtering to help stop unsolicited commercial email (UCE). Anti-spam tools should be adaptive to new spam and customized for each site's email patterns. This easy to use tool works with any mail transport and achieves these goals requiring no operator intervention after the initial setup phase.

### 3. ScanADS – Scan Alternate Data Streams v1.1

by Tiago Halm

Relevant URL:

<http://www.kodeit.org/utis/scanads.htm>

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

Summary:

Scans Alternate Data Streams (ADS) in a local/remote system. Files and directories can have several kinds of ADS, some of which are not visible by normal means. These types of streams are not detectable by the "traditional" dir command and its space (bytes occupied) are not reflected in disk space usage reports.

## VI. SPONSOR INFORMATION

---

This Issue is Sponsored by: KaVoDo

Your network Firewall and IDS products do not prevent Web application exploits – the most common form of online attack – resulting in Web defacement, data theft, sabotage and fraud.

KaVaDo is the first and only company that provides a complete and an integrated suite of Web application security products, allowing you to assess your entire environment, automatically set positive security policies and maintain it without compromising business performance.

For more information on KaVaDo and to download a FREE white paper on Web applications – security policy automation, please visit <http://www.securityfocus.com/Kavado-ms-secnews2>

---

---

---