

# SecurityFocus Microsoft Newsletter #228

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-02/0068.html>

---

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

**Date:** 02/16/05

Date: Wed, 16 Feb 2005 14:45:17 -0700 (MST)

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

SecurityFocus Microsoft Newsletter #228

---

Need to know what's happening on YOUR network? Symantec DeepSight Analyzer is a free service that gives you the ability to track and manage attacks. Analyzer automatically correlates attacks from various Firewall and network based Intrusion Detection Systems, giving you a comprehensive view of your computer or general network. Sign up today!

[http://www.securityfocus.com/sponsor/Symantec\\_sf-news\\_041130](http://www.securityfocus.com/sponsor/Symantec_sf-news_041130)

---

## I. FRONT AND CENTER

1. Windows NTFS Alternate Data Streams
2. More Advisories, More Security

## II. MICROSOFT VULNERABILITY SUMMARY

1. RaidenHTTPD Remote File Disclosure Vulnerability
2. Foxmail MAIL-FROM Remote Buffer Overflow Vulnerability
3. Microsoft Outlook Web Access Login Form Remote URI Redirecti...
4. Multiple Web Browser International Domain Name Handling Site...
5. Mozilla Firefox About Configuration Hidden Frame Remote Conf...
6. Mozilla Firefox Drag And Drop Security Policy Bypass Vulnera...
7. Microsoft Internet Explorer URI Decoding Vulnerability
8. Microsoft Internet Explorer DHTML Method Buffer Overflow Vul...
9. Microsoft Windows SharePoint Services Cross-Site Scripting a...
10. Microsoft Internet Explorer Unspecified ActiveX Image Contro...
11. Microsoft Windows Hyperlink Object Library Buffer Overflow V...
12. Microsoft Office XP HTML Link Processing Remote Buffer Overf...
13. Microsoft Windows License Logging Service Buffer Overflow Vu...
14. Microsoft Windows COM Structured Storage Local Privilege Esc...
15. Microsoft Windows Server Message Block Handlers Remote Buffe...
16. Microsoft Windows Media Player Remote PNG Image Format Buffe...
17. Microsoft Windows Named Pipe Remote Information Disclosure V...
18. Microsoft OLE Remote Buffer Overflow Vulnerability
19. XGB Authentication Bypass Vulnerability
20. SafeNet SoftRemote VPN Client Local Password Disclosure Vuln...
21. BrightStor ARCserve/Enterprise Backup UDP Probe Remote Buffe...
22. Symantec UPX Parsing Engine Remote Heap Overflow Vulnerabili...

23. Software602 602 Lan Suite Arbitrary File Upload Vulnerabil...
24. ArGoSoft Mail Server Multiple Directory Traversal Vulnerabil...
25. Microsoft MSN Messenger/Windows Messenger PNG Buffer Overflo...
26. IBM DB2 Universal Database Server Network Message Processing...
27. IBM DB2 Universal Database Server Object Creation Remote Cod...
28. Armagetron Advanced Multiple Remote Denial Of Service Vulner...
29. Microsoft Internet Explorer Multiple Vulnerabilities
30. Zone Labs ZoneAlarm Local Denial of Service Vulnerability

### III. MICROSOFT FOCUS LIST SUMMARY

1. active directory password policy (Thread)
2. Password Protected Screen Saver and AdministrativePa... (Thread)
3. SAM encrypted with syskey (Thread)
4. Password Protected Screen Saver and Administrative P... (Thread)
5. Re[2]: disclosure the administrative password (Thread)
6. SecurityFocus Microsoft Newsletter #227 (Thread)
7. disclosure the administrative password (Thread)
8. ISA Server/WWW Blacklist (Thread)

### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. CoreGuard Core Security System
2. KeyCaptor Keylogger
3. SpyBuster
4. FreezeX
5. NeoExec for Active Directory
6. Secrets Protector v2.03

### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. SafeLogon 2.0
2. SafeSystem 1.5
3. SQL column finder 0.1
4. Secure Hive 1.0.0.1
5. SigupShield 3.0
6. PE Explorer 1.96

### VI. UNSUBSCRIBE INSTRUCTIONS

### VII. SPONSOR INFORMATION

#### I. FRONT AND CENTER

---

##### 1. Windows NTFS Alternate Data Streams

by Don Parker

The purpose of this article is to explain the existence of alternate data streams in Microsoft Windows, demonstrate how to create them by compromising a machine using the Metasploit Framework, and then use freeware tools to easily discover these hidden files.

<http://www.securityfocus.com/infocus/1822>

##### 2. More Advisories, More Security

By Thierry Carrez

More and more, we see articles questioning the security of a given platform based solely on the number of advisories published -- and this approach is simply wrong.

<http://www.securityfocus.com/columnists/299>

## II. MICROSOFT VULNERABILITY SUMMARY

---

### 1. RaidenHTTPD Remote File Disclosure Vulnerability

BugTraq ID: 12451

Remote: Yes

Date Published: Feb 05 2005

Relevant URL: <http://www.securityfocus.com/bid/12451>

Summary:

RaidenHTTPD is reported prone to a remote file disclosure vulnerability. It is reported that the service does not correctly handle requests for restricted files that reside outside of the web document root folder.

A remote attacker may exploit this issue to disclose the contents of web server readable files.

### 2. Foxmail MAIL-FROM Remote Buffer Overflow Vulnerability

BugTraq ID: 12454

Remote: Yes

Date Published: Feb 05 2005

Relevant URL: <http://www.securityfocus.com/bid/12454>

Summary:

It is reported that Foxmail server is prone to a remote buffer overflow vulnerability. This issue is due to a failure of the application to verify buffer boundaries when processing user-supplied email headers.

A remote attacker may potentially exploit this issue to cause the email server to crash, denying service to legitimate users. It is also possible to further leverage this issue in order to execute arbitrary code; this code would be executed in the security context of the affected service.

### 3. Microsoft Outlook Web Access Login Form Remote URI Redirecti...

BugTraq ID: 12459

Remote: Yes

Date Published: Feb 07 2005

Relevant URL: <http://www.securityfocus.com/bid/12459>

Summary:

A remote URI redirection vulnerability affects Microsoft Outlook Web Access. This issue is due to a failure of the application to properly sanitize URI supplied data.

An attacker may leverage this issue to carry out convincing phishing attacks against unsuspecting users by causing an arbitrary page to be loaded once the Microsoft Outlook Web Access login form is submitted.

### 4. Multiple Web Browser International Domain Name Handling Site...

BugTraq ID: 12461

Remote: Yes

Date Published: Feb 07 2005

Relevant URL: <http://www.securityfocus.com/bid/12461>

Summary:

Multiple Web browsers are reported prone to vulnerabilities that surround the handling of International Domain Names.

The vulnerabilities exist due to inconsistencies in how International Domain Names are processed. Reports indicate that this inconsistency can be leveraged to spoof address bar, status-bar, and SSL certificate values.

These vulnerabilities may be exploited by a remote attacker to aid in phishing style attacks. This may result in the voluntary disclosure of sensitive information to a malicious website due to a false sense of trust.

Although these vulnerabilities are reported to affect Web browsers, mail clients that depend on the Web browser to generate HTML code may also be affected.

#### 5. Mozilla Firefox About Configuration Hidden Frame Remote Conf...

BugTraq ID: 12466

Remote: Yes

Date Published: Feb 07 2005

Relevant URL: <http://www.securityfocus.com/bid/12466>

Summary:

A remote configuration manipulation vulnerability affects Mozilla Firefox. This issue is due to a failure of the application to properly secure sensitive configuration scripts from being activated by remote attackers.

An attacker may leverage this issue to alter an unsuspecting user's configuration settings; this may lead to a false sense of security as sensitive settings may be manipulated without the user's knowledge.

#### 6. Mozilla Firefox Drag And Drop Security Policy Bypass Vulnera...

BugTraq ID: 12468

Remote: Yes

Date Published: Feb 07 2005

Relevant URL: <http://www.securityfocus.com/bid/12468>

Summary:

Mozilla Firefox is reported prone to a security vulnerability that could allow a malicious website to bypass drag-and-drop functionality security policies.

It is demonstrated that it is possible to exploit this vulnerability with an image that renders correctly in the Firefox browser but that, when dragged and dropped onto the local file system, will be saved with a '.bat' file extension.

Because the batch file interpreter on Microsoft Windows is particularly lenient when it comes to syntax, batch commands appended to the image file will be executed if the image that was dragged and dropped is invoked.

Update: Netscape 7.2 is reported vulnerable to this issue as well. It is possible that other versions may also be affected.

#### 7. Microsoft Internet Explorer URI Decoding Vulnerability

BugTraq ID: 12473

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12473>

Summary:

Microsoft Internet Explorer is prone to a vulnerability related to URI decoding.

A bug in how the browser parses encoded URI data may allow zone bypass. As a result, it is possible to force the browser to interpret Web content in the Local Zone. This could be exploited to execute arbitrary code in the context of the user who is currently logged in.

Cross-site scripting attacks are also possible due to this issue, as well as partial address bar obfuscation.

This vulnerability is similar to the zone bypass attack described in BID 10517.

8. Microsoft Internet Explorer DHTML Method Buffer Overflow Vul...

BugTraq ID: 12475

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12475>

Summary:

Microsoft Internet Explorer is prone to a heap-based buffer overflow vulnerability. This vulnerability is due to a boundary condition error that is exposed when passing data to the 'createControlRange()' DHTML method, resulting in corruption of heap-based memory with attacker-supplied data.

This vulnerability could be exploited to execute arbitrary code in the context of the currently logged in user.

9. Microsoft Windows SharePoint Services Cross-Site Scripting a...

BugTraq ID: 12476

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12476>

Summary:

A cross-site scripting and spoofing vulnerability affects Microsoft Windows SharePoint Services and SharePoint Team Services.

A remote attacker may carry out a cross-site scripting attack to execute arbitrary HTML and script code in a user's browser. It is also possible to poison Web browser and intermediate proxy server caches by placing spoofed content in the caches.

10. Microsoft Internet Explorer Unspecified ActiveX Image Contro...

BugTraq ID: 12477

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12477>

Summary:

Microsoft has announced in the MS05-014 Cumulative Internet Explorer bulletin that the ActiveX Image Control 1.0 is no longer supported due to an unspecified security vulnerability. The cumulative update addresses the vulnerability by setting the kill-bit on the control so that it may no longer be invoked from Internet Explorer.

The impact of this unspecified vulnerability is not known at this time.

11. Microsoft Windows Hyperlink Object Library Buffer Overflow V...

BugTraq ID: 12479

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12479>

Summary:

The Microsoft Windows Hyperlink Object Library is reported prone to a buffer overflow vulnerability. An attacker may exploit this condition to execute arbitrary code on a vulnerable computer, which may grant unauthorized access to the computer or lead to privilege escalation.

It is reported that issue presents itself when a user follows a malformed link specially crafted by an attacker, however, other attack vectors also exist to exploit this vulnerability. Specifically, an application that employs the affected library by accepting and supplying parameters to the library may allow an attacker to exploit this vulnerability remotely and without user interaction.

Local attacker vectors exist to exploit this vulnerability as well. Reportedly, an attacker with local interactive access to a vulnerable computer may pass a malicious payload to an application that supplies parameters to the affected library.

#### 12. Microsoft Office XP HTML Link Processing Remote Buffer Overf...

BugTraq ID: 12480

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12480>

Summary:

A remote buffer overflow vulnerability affects Microsoft Office XP. The problem presents itself when an unsuspecting user follows a malicious HTML link that points to a Office document. A boundary condition error is exposed during this operation that may allow attacker-specified data to corrupt process memory.

An attacker may leverage this issue to execute arbitrary code with the privileges of an unsuspecting user that follows a malicious embedded link.

#### 13. Microsoft Windows License Logging Service Buffer Overflow Vu...

BugTraq ID: 12481

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12481>

Summary:

A buffer overflow exists in the Microsoft Windows License Logging Service. This could allow remote execution of arbitrary code.

#### 14. Microsoft Windows COM Structured Storage Local Privilege Esc...

BugTraq ID: 12483

Remote: No

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12483>

Summary:

Microsoft Windows is reported prone to a local privilege escalation vulnerability when processing COM structured storage files. This issue may allow a local attacker to gain elevated privileges on a vulnerable computer.

An attacker with local interactive access may craft an application that triggers this condition and gain SYSTEM privileges on a vulnerable computer.

#### 15. Microsoft Windows Server Message Block Handlers Remote Buffe...

BugTraq ID: 12484

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12484>

Summary:

Microsoft Windows Server Message Block handler is reported prone to a remote buffer overflow

vulnerability.

It should be noted that SMB drivers execute in the kernel memory space and a successful attack can allow a remote attacker to gain unauthorized access with ring 0 privileges.

Microsoft has noted that other protocols, such as IPX/SPX, could also be vulnerable to this issue.

#### 16. Microsoft Windows Media Player Remote PNG Image Format Buffe...

BugTraq ID: 12485

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12485>

Summary:

A remote buffer overflow vulnerability affects the Portable Network Graphics (PNG) image format processing functionality of Microsoft Windows Media Player. This issue is due to a failure of the application to properly validate the size of image data prior to copying it into static process buffers.

An attacker may exploit this issue to execute arbitrary code with the privileges of the SYSTEM user. This will facilitate unauthorized access and privilege escalation.

#### 17. Microsoft Windows Named Pipe Remote Information Disclosure V...

BugTraq ID: 12486

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12486>

Summary:

A remote information disclosure vulnerability affects Microsoft Windows. This issue is due to a failure of the application to securely store potentially sensitive system information.

An attacker may leverage this issue to disclose the user names of all users connected to a network share, potentially facilitating further attacks against affected computers.

#### 18. Microsoft OLE Remote Buffer Overflow Vulnerability

BugTraq ID: 12488

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12488>

Summary:

Microsoft OLE is reported prone to a remote buffer overflow vulnerability. This issue arises because the application fails to perform boundary checks before copying user-supplied data to sensitive process buffers. A remote attacker may leverage this vulnerability to execute arbitrary code on a vulnerable computer.

If a vulnerable user opens a malicious file through any application that supports OLE, the attacker-supplied arbitrary code may be executed in the context of the user.

Reportedly, user interaction is required to exploit this condition in Microsoft Windows 2000, Windows XP, and Windows Server 2003.

An anonymous remote user can exploit this issue in various versions of Microsoft Exchange Server because Exchange Server uses the affected Windows OLE component. A successful attack can allow the attacker to gain SYSTEM privileges as the Microsoft Exchange Server runs with elevated privileges. Affected Microsoft

## SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #228

Exchange Server versions include Microsoft Exchange 2000 Server, Microsoft Exchange Server 2003, Microsoft Exchange Server 5.0, and Microsoft Exchange Server 5.5.

Other applications that use the affected Windows OLE component include Microsoft Office XP Service Pack 3, Microsoft Office XP Service Pack 2, Microsoft Office 2003 Service Pack 1, and Microsoft Office 2003.

### 19. XGB Authentication Bypass Vulnerability

BugTraq ID: 12489

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12489>

Summary:

xGB is reportedly affected by a vulnerability that could permit unauthorized administrator access. This issue is due to the application failing to properly verify user credentials.

A malicious user could exploit this vulnerability to bypass user authentication and gain administrative access.

This vulnerability is reported to affect xGB version 2.0; earlier versions may also be vulnerable.

### 20. SafeNet SoftRemote VPN Client Local Password Disclosure Vuln...

BugTraq ID: 12490

Remote: No

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12490>

Summary:

SoftRemote and SoftRemoteLT VPN client utilities are reported prone to a local pre-shared key (password) disclosure vulnerability. It is reported that the VPN password is stored in the memory image of the process in plain-text format.

Credentials that are harvested through the exploitation of this vulnerability may then be used to aid in further attacks.

### 21. BrightStor ARCserve/Enterprise Backup UDP Probe Remote Buffe...

BugTraq ID: 12491

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12491>

Summary:

Various Computer Associates BrightStor ARCserve/Enterprise Backup products are prone to a remote buffer overflow vulnerability. This issue presents itself because the affected applications do not perform boundary checks prior to copying user-supplied data into sensitive process buffers.

A remote attacker may execute arbitrary code on a vulnerable computer to gain unauthorized access to it.

### 22. Symantec UPX Parsing Engine Remote Heap Overflow Vulnerabili...

BugTraq ID: 12492

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12492>

Summary:

Various Symantec products are reported prone to a remote heap overflow vulnerability. This issue affects the

UPX Parsing Engine shipped with the products.

A successful attack may allow a remote attacker to execute arbitrary code on a vulnerable computer leading to a complete compromise.

23. Software602 602 Lan Suite Arbitrary File Upload Vulnerabilit...

BugTraq ID: 12495

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12495>

Summary:

602 Lan Suite 2004 is reportedly affected by a vulnerability regarding the uploading of file attachments. This issue is due to the application failing to properly sanitize the names of file attachments before upload. A malicious user could exploit this vulnerability using directory traversal attacks to upload a file to an arbitrary location accessible by the affected server.

This vulnerability could lead to the execution of a malicious file on the server hosting the application.

602 Lan Suite 2004 version 2004.0.04.1221 is reportedly vulnerable; other versions may also be affected.

24. ArGoSoft Mail Server Multiple Directory Traversal Vulnerabil...

BugTraq ID: 12502

Remote: Yes

Date Published: Feb 09 2005

Relevant URL: <http://www.securityfocus.com/bid/12502>

Summary:

ArGoSoft Mail Server is reported prone to multiple directory traversal vulnerabilities. These issues result from insufficient sanitization of user-supplied data and may allow remote attackers to view, replace and delete arbitrary files, folders, and users' email on a vulnerable computer running the server.

ArGoSoft Mail Server 1.8.7.3 is reported vulnerable to these issues. It is possible that prior versions are affected as well.

25. Microsoft MSN Messenger/Windows Messenger PNG Buffer Overflo...

BugTraq ID: 12506

Remote: Yes

Date Published: Feb 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12506>

Summary:

A remotely exploitable buffer overflow exists in MSN Messenger and Windows Messenger. This vulnerability is related to parsing of Portable Network Graphics (PNG) image header data. Successful exploitation will result in execution of arbitrary code in the context of the vulnerable client user.

Attack vectors and mitigations may differ for MSN Messenger and Windows Messenger. For Windows Messenger, the attacker must spoof the .NET Messenger service and the client must be configured to receive .NET alerts.

However, MSN Messenger may be exploited through various methods in a client-to-client attack. Possible attack vectors for this vulnerability in MSN Messenger include:

User display pictures

Custom icons that are displayed inline in instant messages

Thumbnails of transferred images  
Background images

Since this issue may be exploited in a client-to-client attack for MSN Messenger, it is a likely candidate for development of a worm.

This issue was originally described in BID 10857. Further analysis has determined that there are unique properties of the vulnerability that distinguish it from the general libpng issue on other platforms.

#### 26. IBM DB2 Universal Database Server Network Message Processing...

BugTraq ID: 12511

Remote: Yes

Date Published: Feb 10 2005

Relevant URL: <http://www.securityfocus.com/bid/12511>

Summary:

A remote code execution vulnerability affects IBM DB2 Universal Database Server. This issue is due to a failure of the application to properly handle network messages under certain circumstances.

This issue may be related to BID 12508 IBM DB2 Universal Database Unspecified Vulnerability.

An attacker with a database connection may leverage this issue to execute arbitrary code within the context of the affected database instance, potentially facilitating unauthorized access or privilege escalation.

#### 27. IBM DB2 Universal Database Server Object Creation Remote Cod...

BugTraq ID: 12514

Remote: Yes

Date Published: Feb 10 2005

Relevant URL: <http://www.securityfocus.com/bid/12514>

Summary:

A remote code execution vulnerability affects IBM DB2 Universal Database Server. This issue is due to a failure of the application to properly handle the creation of new objects.

This issue may be related to BID 12508 IBM DB2 Universal Database Unspecified Vulnerability.

An attacker with a database connection may leverage this issue to execute arbitrary code within the context of the affected database instance, potentially facilitating unauthorized access or privilege escalation.

#### 28. Armagetron Advanced Multiple Remote Denial Of Service Vulner...

BugTraq ID: 12520

Remote: Yes

Date Published: Feb 10 2005

Relevant URL: <http://www.securityfocus.com/bid/12520>

Summary:

Multiple denial of service vulnerabilities affect Armagetron Advanced. These issues are due to a failure of the application to handle malformed network data.

An attacker may leverage these issues to cause a remote denial of service condition in affected applications.

#### 29. Microsoft Internet Explorer Multiple Vulnerabilities

BugTraq ID: 12530

Remote: Yes

## SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #228

Date Published: Feb 11 2005

Relevant URL: <http://www.securityfocus.com/bid/12530>

Summary:

Microsoft Internet Explorer is reported prone to multiple vulnerabilities. These issues may allow remote attackers to execute arbitrary script code, disclose sensitive information and execute files from the local system. These issues are alleged to have been addressed by MS05-014.

The following specific issues were identified:

The first issue may allow remote attackers to place arbitrary files on a vulnerable computer. It is possible that this issue is related to BID 10973 (Microsoft Internet Explorer Implicit Drag and Drop File Installation Vulnerability) and BID 11466 (Microsoft Internet Explorer Valid File Drag and Drop Embedded Code Vulnerability). It is not known if this variant is distinct from other known issues

The browser is reported prone to another cross-zone scripting vulnerability. It is reported that an attacker can link to local resources by crafting a malicious Web site and enticing a user to visit the site. This issue is triggered when the user clicks on the attacker's site.

Another issue affecting the application allows malicious Web sites to reference sites from the 'Temporary Internet Files' folder.

The application is prone to a vulnerability that may allow attackers to execute files from the Local zone.

These issues may be combined to ultimately execute arbitrary code in the Local zone. This can lead to unauthorized access to the vulnerable computer.

Internet Explorer 5.01 and 5.5 have been reported vulnerable as well.

This BID will be divided into individual BIDs and updated when further analysis is complete.

30. Zone Labs ZoneAlarm Local Denial of Service Vulnerability

BugTraq ID: 12531

Remote: No

Date Published: Feb 11 2005

Relevant URL: <http://www.securityfocus.com/bid/12531>

Summary:

Multiple ZoneAlarm products and Check Point Integrity Client are reported prone to a local denial of service vulnerability. This issue exists due to an invalid pointer dereference.

A successful attack can result in a denial of service condition in the kernel.

ZoneAlarm Security Suite, ZoneAlarm Pro, and ZoneAlarm versions prior to 5.5.062.011 and Check Point Integrity Client versions prior to 4.5.122.000 and 5.1.556.166 are considered vulnerable to this issue.

### III. MICROSOFT FOCUS LIST SUMMARY

---

1. active directory password policy (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/390379>

2. Password Protected Screen Saver and AdministrativePa... (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/390119>

3. SAM encrypted with syskey (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/390111>

4. Password Protected Screen Saver and Administrative P... (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/390095>

5. Re[2]: disclosure the administrative password (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/389978>

6. SecurityFocus Microsoft Newsletter #227 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/389901>

7. disclosure the administrative password (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/389782>

8. ISA Server/WWW Blacklist (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/389765>

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

---

1. CoreGuard Core Security System

By: Vormetric

Platforms: AIX, Linux, Solaris, Windows 2000, Windows XP

Relevant URL: <http://www.vormetric.com/products/#overview>

Summary:

CoreGuard System profile

The CoreGuard System is the industry's first solution that enforces acceptable use policy for sensitive digital information assets and protects personal data privacy across an enterprise IT environment. CoreGuard's innovative architecture and completeness of technology provide a comprehensive, extensible solution that tightly integrates all the elements required to protect information across a widespread,

heterogeneous enterprise network, while enforcing separation of duties between security and IT administration. At the same time, CoreGuard is transparent to users, applications and storage infrastructures for ease of deployment and system management.

CoreGuard enables customers to:

- \* Protect customer personal data privacy and digital information assets
- \* Protect data at rest from unauthorized viewing by external attackers and unauthorized insiders
- \* Enforce segregation of duties between IT administrators and security administration
- \* Ensure host & application integrity \* Block malicious code, including zero-day exploits

## 2. KeyCaptor Keylogger

By: Keylogger Software

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

Relevant URL: <http://www.keylogger-software.com/keylogger/keylogger.htm>

Summary:

KeyCaptor is your solution for recording ALL keystrokes of ALL users on your computer! Now you have the power to record emails, websites, documents, chats, instant messages, usernames, passwords, and MUCH MORE!

With our advanced stealth technology, KeyCaptor will not show in your processes list and cannot be stopped from running unless you say so!

## 3. SpyBuster

By: Remove Spyware

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

Relevant URL: <http://www.remove-spyware.com/spybuster.htm>

Summary:

Our award winning spyware / adware scanner and removal software, SpyBuster will scan your computer for over 4,000 known spyware and adware applications. SpyBuster protects your computer from data stealing programs that can expose your personal information.

SpyBuster scanning technology allows for a quick and easy sweep, so you can resume your work in minutes.

## 4. FreezeX

By: Faronics Technologies USA Inc

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

Relevant URL: <http://www.faronics.com/html/Freezex.asp>

Summary:

FreezeX prevents all unauthorized programs, including viruses, keyloggers and spy ware from executing. Powerful and secure, FreezeX ensures that any new executable, program, or application that is downloaded, introduced via removable media or the network will never install

## 5. NeoExec for Active Directory

By: NeoValens

Platforms: Windows 2000, Windows XP

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

Summary:

NeoExec® is an operating system extension for Windows 2000/XP that allows the setting of privileges at the application level rather than at the user level.

NeoExec® is the ideal solution for applications that require elevated privileges to run as the privileges are granted to the application, not the user.

NeoExec® is the only solution on the market capable of modifying at runtime the processes' security context — without requiring a second account as with RunAs and RunAs-derived products.

#### 6. Secrets Protector v2.03

By: E-CRONIS

Platforms: Windows 2000, Windows XP

Relevant URL: <http://www.e-cronis.com/download/sp.exe>

Summary:

It's the end of your worries about top-secret data of your company, your confidential files or the pictures from the last party. All these will be hidden beyond the reach of ANY intruder and you will be the only one able to handle them. And what you want to delete will be DELETED. It is the ultimate security tool to protect your sensitive information on PC, meeting the three most important security issues: Integrity, Confidentiality and Availability. This product gives you the features of a "folder locker" and a "secure eraser".

Your secret information is available only through this software and there is no other mean to access it. The information is protected at file system level and it cannot be accidentally deleted or overwritten neither in Safe mode nor in other operating system. This program doesn't make your operating system unstable as other related product do and protects your information from being seen, altered or deleted by an unauthorized user with or without his wish. The program allows you to permanently erase your sensitive data using secure wiping methods leaving no trace of your information. Depending on the selected wiping method your data is unrecoverable using software or even hardware recovery techniques.

### V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

#### 1. SafeLogon 2.0

By: GemiScorp Software Solutions

Relevant URL: <http://www.gemiscorp.com/english/slogon/info.html>

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

Summary:

SafeLogon is a multi-user and password-based access control utility that enhances and complements the Windows built-in logon and authentication system. In other words, SafeLogon allows you to protect your system at home and office from unauthorized access.

SafeLogon is fully configurable and allows its Administrator to:

- Restrict access to Windows to certain users, optionally controlling the days of the week and the time of the day the user is allowed to log on and

## 2. SafeSystem 1.5

By: GemiScorp Software Solutions

Relevant URL: <http://www.gemiscorp.com/english/safesystem/info.html>

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

Summary:

SafeSystem is a security program that allows you to prevent access to your personal and important files and folders, as well as protect and guarantee the integrity and well functioning of your system. SafeSystem can make your files and folders completely invisible, inaccessible or simply read-only. Furthermore, SafeSystem can prevent the change of configuration and the accidental (or even intentional) system files deletion or alteration, so your PC will be healthy

## 3. SQL column finder 0.1

By: Rafal Bielecki

Relevant URL: <http://sqlcfind.netro.pl/sqlcfind.exe>

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

Summary:

Helps you to find exact columns number when using union select query

## 4. Secure Hive 1.0.0.1

By: Secure Hive

Relevant URL: <http://www.securehive.com/Secure%20Hive.htm>

Platforms: Windows 2000, Windows NT, Windows XP

Summary:

What Does Secure Hive Enterprise Offer?

Encryption of part, or entire, Word documents, Excel worksheets or PowerPoint presentations through Secure Hive's integration with Microsoft Office.

Encryption of part, or entire, content of common documents (such as Notepad, WordPad), email messages and instant messages, including mixed text and graphics, with Secure Hive's Clipboard Encryption feature.

## 5. SignupShield 3.0

By: Protecteer, LLC

Relevant URL: <http://www.protecteer.com/install3/full/sus.exe>

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

Summary:

A fraud alert (Anti-Phishing) software integrated with a full life-cycle password manager & form filler. SignupShield generates unlimited number of unique passwords and disposable email addresses for signing-up to web sites.

It fills sign-up forms and encrypts passwords and email addresses for later use during sign-in.

## 6. PE Explorer 1.96

By: Heaventools Software

Relevant URL: <http://www.heaventools.com/overview.htm>

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

Summary:

PE Explorer is a tool for inspecting and editing the inner workings of Windows 32-bit executable files. It offers a look at PE file structure and all of the resources in the file, and reports multiple details about a PE file (EXE, DLL, ActiveX controls, and several other Windows executable formats). Once inside, file structure can be analyzed and optimized, hostile code detected, spyware tracked down, problems diagnosed, changes made and resources repaired.

#### VI. UNSUBSCRIBE INSTRUCTIONS

---

To unsubscribe send an e-mail message to [ms-secnews-unsubscribe@securityfocus.com](mailto:ms-secnews-unsubscribe@securityfocus.com) from the subscribed address. The contents of the subject or message body do not matter. You will receive a confirmation request message to which you will have to answer. Alternatively you can also visit <http://www.securityfocus.com/newsletters> and unsubscribe via the website.

If your email address has changed email [listadmin@securityfocus.com](mailto:listadmin@securityfocus.com) and ask to be manually removed.

#### VII. SPONSOR INFORMATION

---

Need to know what's happening on YOUR network? Symantec DeepSight Analyzer is a free service that gives you the ability to track and manage attacks. Analyzer automatically correlates attacks from various Firewall and network based Intrusion Detection Systems, giving you a comprehensive view of your computer or general network. Sign up today!

[http://www.securityfocus.com/sponsor/Symantec\\_sf-news\\_041130](http://www.securityfocus.com/sponsor/Symantec_sf-news_041130)

---

---

---