

SecurityFocus Microsoft Newsletter #229

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-02/0073.html>

From: Marc Fossi (mfossi_at_securityfocus.com)

Date: 02/23/05

Date: Tue, 22 Feb 2005 18:09:01 -0700 (MST)

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

SecurityFocus Microsoft Newsletter #229

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

I. FRONT AND CENTER

1. Complexity Kills Innovation
2. Windows NTFS Alternate Data Streams

II. MICROSOFT VULNERABILITY SUMMARY

1. BrightStor ARCserve/Enterprise Discovery Service SERVICEPC R...
2. IBM WebSphere Application Server JSP Engine Source Code Disc...
3. IBM WebSphere Application Server File Servlet Source Code Di...
4. Microsoft Internet Explorer Mouse Event URI Status Bar Obfus...
5. VBulletin Forumdisplay.PHP Remote Command Execution Vulnerab...
6. AWStats Plugin Multiple Remote Command Execution Vulnerabili...
7. Microsoft Internet Explorer Favorites List Script Code Execu...
8. AWStats Debug Remote Information Disclosure Vulnerability
9. Opera Web Browser Multiple Remote Vulnerabilities
10. CitrusDB CSV File Upload Access Validation Vulnerability
11. KarjaSoft Sami HTTP Server Multiple Remote Vulnerabilities
12. CitrusDB Remote Authentication Bypass Vulnerability
13. PHP-Nuke Multiple Cross-Site Scripting Vulnerabilities
14. CitrusDB Arbitrary Local PHP File Include Vulnerability
15. Microsoft Internet Explorer Malformed File URI Denial of Ser...
16. AWStats Logfile Parameter Remote Command Execution Vulnerabi...
17. Microsoft ASP.NET Unicode Character Conversion Multiple Cros...
18. Yahoo! Messenger Local Insecure Default Installation Vulnera...
19. Yahoo! Messenger Download Dialogue Box File Name Spoofing Vu...
20. Tarantella Enterprise/Secure Global Desktop Remote Informati...

III. MICROSOFT FOCUS LIST SUMMARY

1. SecurityFocus Microsoft Newsletter #228 (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. Complexity Kills Innovation

By Kelly Martin

There's more innovation coming from today's virus writers than from the big software companies whose core goals are to progress and innovate.

<http://www.securityfocus.com/columnists/300>

2. 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>

II. MICROSOFT VULNERABILITY SUMMARY

1. BrightStor ARCserve/Enterprise Discovery Service SERVICEPC R...

BugTraq ID: 12536

Remote: Yes

Date Published: Feb 14 2005

Relevant URL: <http://www.securityfocus.com/bid/12536>

Summary:

A remote buffer overflow vulnerability reportedly affects BrightStor ARCserve/Enterprise. This issue is due to a failure of the application to securely copy data from the network. It should be noted that this issue is reportedly distinct from that outlined in BID 12522 (BrightStor ARCserve/Enterprise Backup UDP Probe Remote Buffer Overflow Vulnerability).

A remote attacker may execute arbitrary code on a vulnerable computer, potentially facilitating unauthorized superuser access. A denial of service condition may arise as well.

2. IBM WebSphere Application Server JSP Engine Source Code Disc...

BugTraq ID: 12537

Remote: Yes

Date Published: Feb 14 2005

Relevant URL: <http://www.securityfocus.com/bid/12537>

Summary:

IBM WebSphere Application Server is prone to a source code disclosure vulnerability. An attacker can exploit this issue by supplying a malformed URI to the server to disclose JSP source code.

It should be noted that this issue only affects WebSphere Application Server versions 5.0 and 5.1 running on Microsoft Windows platforms.

3. IBM WebSphere Application Server File Servlet Source Code Di...

BugTraq ID: 12538

Remote: Yes

Date Published: Feb 14 2005

Relevant URL: <http://www.securityfocus.com/bid/12538>

Summary:

IBM WebSphere Application Server is prone to a source code disclosure vulnerability. An attacker can exploit this issue by supplying a malformed URI to the server to disclose JSP source code. The vulnerability exists in the file serving servlet.

It should be noted that this issue only affects WebSphere Application Server version 6.0 running on Microsoft Windows platforms.

4. Microsoft Internet Explorer Mouse Event URI Status Bar Obfus...

BugTraq ID: 12541

Remote: Yes

Date Published: Feb 14 2005

Relevant URL: <http://www.securityfocus.com/bid/12541>

Summary:

Microsoft Internet Explorer is reported prone to a URI obfuscation weakness.

The issue presents itself when a HREF tag contains certain mouse events.

This issue may be leveraged by an attacker to display false information in the status bar or URI property dialog of an affected browser, allowing an attacker to present web pages to unsuspecting users that seem to originate from a trusted location. This may facilitate phishing style attacks; other attacks may also be possible.

5. VBulletin Forumdisplay.PHP Remote Command Execution Vulnerab...

BugTraq ID: 12542

Remote: Yes

Date Published: Feb 14 2005

Relevant URL: <http://www.securityfocus.com/bid/12542>

Summary:

VBulletin is reported prone to a remote arbitrary command execution vulnerability. This issue presents itself due to insufficient sanitization of user-supplied data and affects the 'forumdisplay.php' script when the 'showforumusers' option has been enabled.

This may allow attackers to execute arbitrary commands with the privileges of the server running the application.

VBulletin versions 3.0 to 3.0.4 are reported vulnerable to this issue. It is reported that versions 3.0.5 and 3.0.6 are not affected.

6. AWStats Plugin Multiple Remote Command Execution Vulnerability

BugTraq ID: 12543

Remote: Yes

Date Published: Feb 14 2005

Relevant URL: <http://www.securityfocus.com/bid/12543>

Summary:

Multiple remote command execution vulnerabilities reportedly affect AWStats. These issues are due to an input validation error that allows a remote attacker to specify commands to be executed in the context of the affected application.

The first problem presents itself due to the potential of malicious use of the 'loadplugin' and 'pluginmode' parameters of the 'awstats.pl' script. The second issue arises from an insecure implementation of the 'loadplugin' parameter functionality.

An attacker may leverage these issues to execute arbitrary commands with the privileges of the affected web server running the vulnerable scripts. This may facilitate unauthorized access to the affected computer, as well as other attacks.

Multiple sources have reported that AWStats 6.3 and subsequent versions are not vulnerable to these issues.

7. Microsoft Internet Explorer Favorites List Script Code Execution Vulnerability

BugTraq ID: 12544

Remote: Yes

Date Published: Feb 14 2005

Relevant URL: <http://www.securityfocus.com/bid/12544>

Summary:

Microsoft Internet Explorer is reported prone to a security vulnerability.

It is alleged that a JavaScript URI may be added to Internet Explorer favorites if the 'CTRL-d' key combination is pressed to bookmark a website that contains a specially crafted pop-up window.

This vulnerability may be harnessed to aid in the exploitation of other vulnerabilities.

8. AWStats Debug Remote Information Disclosure Vulnerability

BugTraq ID: 12545

Remote: Yes

Date Published: Feb 14 2005

Relevant URL: <http://www.securityfocus.com/bid/12545>

Summary:

A remote information disclosure vulnerability reportedly affects AWStats. This issue is due to a failure of the application to properly validate access to sensitive data.

An attacker may leverage this issue to gain access to potentially sensitive data, possibly facilitating further attacks against an affected computer.

9. Opera Web Browser Multiple Remote Vulnerabilities

BugTraq ID: 12550

Remote: Yes

Date Published: Feb 14 2005

Relevant URL: <http://www.securityfocus.com/bid/12550>

Summary:

Opera Web Browser is reported prone to multiple vulnerabilities that are exploitable remotely. The following issues are reported:

Opera Web Browser is prone to a vulnerability that presents itself when the browser handles 'data' URIs.

A remote malicious website may exploit this condition to execute arbitrary code in the context of a user that is running a vulnerable version of the affected browser.

Opera Web Browser is prone to an unspecified security vulnerability that exists in the Opera Java LiveConnect class.

Few details are known in regards to this vulnerability. However, it is believed that the issue may be exploited by a remote malicious web site to access dangerous private Java methods. This is not confirmed.

This BID will be updated as soon as further research into these issues is completed.

10. CitrusDB CSV File Upload Access Validation Vulnerability

BugTraq ID: 12557

Remote: Yes

Date Published: Feb 15 2005

Relevant URL: <http://www.securityfocus.com/bid/12557>

Summary:

CitrusDB is reportedly affected by an access validation vulnerability during the upload of CSV files. Exploitation of this issue could result in path disclosure or SQL injection. The issue exists because the application fails to verify user credentials during file upload and import.

These issues are reported to affect CitrusDB 0.3.6; earlier versions may also be affected.

11. KarjaSoft Sami HTTP Server Multiple Remote Vulnerabilities

BugTraq ID: 12559

Remote: Yes

Date Published: Feb 15 2005

Relevant URL: <http://www.securityfocus.com/bid/12559>

Summary:

Multiple remote vulnerabilities affect KarjaSoft Sami HTTP server. These issues are due to poor input validation and a failure to handle malformed network-based requests.

The first issue is a directory traversal issue. The second issue is a denial of service issue.

An attacker may leverage these issues to reveal files outside of the Web server root directory or to crash the affected server.

12. CitrusDB Remote Authentication Bypass Vulnerability

BugTraq ID: 12560

Remote: Yes

Date Published: Feb 15 2005

Relevant URL: <http://www.securityfocus.com/bid/12560>

Summary:

CitrusDB is reportedly affected by an authentication bypass vulnerability. This issue is due to the application using a static value during the creation of user cookie information.

An attacker could exploit this vulnerability to log in as any existing user, including the 'admin' account.

This issue is reported to affect CitrusDB 0.3.6; earlier versions may also be affected.

13. PHP–Nuke Multiple Cross–Site Scripting Vulnerabilities

BugTraq ID: 12561

Remote: Yes

Date Published: Feb 15 2005

Relevant URL: <http://www.securityfocus.com/bid/12561>

Summary:

It is reported that PHP–Nuke is affected by various cross–site scripting vulnerabilities. These issues are due to a failure of the application to properly sanitize user–supplied URI input.

These issues could permit a remote attacker to create a malicious URI link that includes hostile HTML and script code. If this link were to be followed, the hostile code may be rendered in the web browser of the victim user. This would occur in the security context of the affected web site and may allow for theft of cookie–based authentication credentials

14. CitrusDB Arbitrary Local PHP File Include Vulnerability

BugTraq ID: 12564

Remote: Unknown

Date Published: Feb 15 2005

Relevant URL: <http://www.securityfocus.com/bid/12564>

Summary:

CitrusDB is reportedly affected by a vulnerability that permits the inclusion of any local PHP file. This issue is due to the application failing to properly sanitize user–supplied input.

This issue is reported to affect CitrusDB 0.3.6; earlier versions may also be affected.

This issue may also allow remote file includes, although this has not been confirmed.

15. Microsoft Internet Explorer Malformed File URI Denial of Ser...

BugTraq ID: 12565

Remote: Yes

Date Published: Feb 15 2005

Relevant URL: <http://www.securityfocus.com/bid/12565>

Summary:

Microsoft Internet Explorer is reported prone to a remote denial of service vulnerability.

It is reported that the affected browser will crash when a malformed 'file:' URI is processed.

A remote attacker may exploit this vulnerability to crash the affected browser.

16. AWStats Logfile Parameter Remote Command Execution Vulnerabi...

BugTraq ID: 12572

Remote: Yes

Date Published: Feb 16 2005

Relevant URL: <http://www.securityfocus.com/bid/12572>

Summary:

AWStats is reported prone to a remote arbitrary command execution vulnerability. This issue presents itself due to insufficient sanitization of user-supplied data.

Specifically, the user-specified 'logfile' URI parameter is supplied to the Perl open() routine. It is believed that this issue is distinct from BID 10950 (AWStats Rawlog Plugin Logfile Parameter Input Validation Vulnerability).

AWStats versions 5.4 to 6.1 are reported vulnerable to this issue.

17. Microsoft ASP.NET Unicode Character Conversion Multiple Cros...

BugTraq ID: 12574

Remote: Yes

Date Published: Feb 16 2005

Relevant URL: <http://www.securityfocus.com/bid/12574>

Summary:

It is reported that ASP.NET is prone to various cross-site scripting attacks. These issues when ASP.NET converts Unicode characters ranging from U+ff00-U+ff60 to ASCII.

Apparently, the application fails to properly validate Unicode characters allowing an attacker to craft a malicious link containing arbitrary HTML or script code to be executed in a user's browser.

This can facilitate theft of cookie-based credentials and other attacks.

18. Yahoo! Messenger Local Insecure Default Installation Vulnera...

BugTraq ID: 12585

Remote: No

Date Published: Feb 18 2005

Relevant URL: <http://www.securityfocus.com/bid/12585>

Summary:

A local insecure default installation vulnerability affects Yahoo! Messenger. This issue is due to a failure of the application to properly secure directories and executables when installation takes place.

A local attacker may leverage this issue to have arbitrary code executed with the privileges of an unsuspecting user; this may facilitate privileges escalation.

19. Yahoo! Messenger Download Dialogue Box File Name Spoofing Vu...

BugTraq ID: 12587

Remote: Yes

Date Published: Feb 18 2005

Relevant URL: <http://www.securityfocus.com/bid/12587>

Summary:

A remote download dialogue box spoofing vulnerability affects Yahoo! Messenger. This issue is due to a design error that facilitates the spoofing of file names.

An attacker may leverage this issue to spoof downloaded file names to unsuspecting users. This issue may lead to a compromise of the target computer as well as other consequences.

It should be noted that although only Yahoo! Messenger version 6.0.0.1750 is reportedly affected; earlier versions may be affected as well.

20. Tarantella Enterprise/Secure Global Desktop Remote Informati...

BugTraq ID: 12591

Remote: Yes

Date Published: Feb 18 2005

Relevant URL: <http://www.securityfocus.com/bid/12591>

Summary:

Tarantella Enterprise 3 and Secure Global Desktop products are prone to an information disclosure vulnerability. This issue arises from a design error that may allow an attacker to gather sensitive information about a vulnerable computer. Information gathered by exploiting this vulnerability may be used to launch other attacks against a computer.

Specifically, computers running Tarantella Enterprise 3 and Secure Global Desktop products in combination with RSA SecurID and multiple users with the same username are affected.

III. MICROSOFT FOCUS LIST SUMMARY

1. SecurityFocus Microsoft Newsletter #228 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/390652>

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 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 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
