

SecurityFocus Microsoft Newsletter #242

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-05/0048.html>

From: Marc Fossi (mfossi_at_securityfocus.com)

Date: 05/25/05

Date: Wed, 25 May 2005 14:30:28 -0600 (MDT)

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

SecurityFocus Microsoft Newsletter #242

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. Is Deleting Spyware A Crime?

II. MICROSOFT VULNERABILITY SUMMARY

1. PostNuke Blocks Module Directory Traversal Vulnerability
2. MetaCart E-Shop ProductsByCategory.ASP Cross-Site Scripting ...
3. Mozilla Suite And Firefox Multiple Script Manager Security B...
4. Mozilla Suite And Firefox DOM Property Overrides Code Execut...
5. War Times Remote Game Server Denial Of Service Vulnerability
6. Fastream NETFile FTP/Web Server FTP Bounce Vulnerability
7. IgnitionServer Entry Deletion Access Validation Checking Vul...
8. IgnitionServer Locked Channel Protected Operator Lockout Vul...
9. Microsoft IPV6 TCPIP Loopback LAND Denial of Service Vulnera...
10. MySQL mysql_install_db Insecure Temporary File Creation Vuln...
11. Microsoft HTML Help Workshop HHC.EXE HHA.DLL HHC Path Memory...
12. Avast! Antivirus Unspecified Scan Evasion Vulnerability
13. Multiple Vendor TCP Timestamp PAWS Remote Denial Of Service ...
14. Microsoft Outlook HTML Email URI Spoofing Vulnerability
15. Groove Networks Groove Virtual Office File Extension Obfusca...
16. Groove Networks Groove Virtual Office SharePoint Lists Arbit...
17. Groove Networks Groove Virtual Office COM Object Security By...
18. Microsoft Word MCW File Handler Buffer Overflow Vulnerabilit...
19. Groove Networks Groove Mobile Workspace SharePoint Lists Arb...
20. NetWin SurgeMail Multiple Unspecified Input Validation Vulne...
21. ImageMagick And GraphicsMagick XWD Decoder Denial Of Service...

III. MICROSOFT FOCUS LIST SUMMARY

1. Encrypting remote files with EFS (Thread)
 2. SecurityFocus Microsoft Newsletter #241 (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. tcpdump for Windows 1.0 beta
2. Assimilator 1.0.0
3. Cenzic Hailstorm 2.0
4. VForce 2.1.008
5. Multiple Interface Watcher 1.0
6. LC 5 5

VI. UNSUBSCRIBE INSTRUCTIONS

VII. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Is Deleting Spyware A Crime?

By Mark Rasch

The murky waters that sustain the spyware companies may have a few unpleasant surprises just beneath the surface.

<http://www.securityfocus.com/columnists/329>

II. MICROSOFT VULNERABILITY SUMMARY

1. PostNuke Blocks Module Directory Traversal Vulnerability

BugTraq ID: 13636

Remote: Yes

Date Published: May 16 2005

Relevant URL: <http://www.securityfocus.com/bid/13636>

Summary:

PostNuke Blocks module is affected by a directory traversal vulnerability.

The problem presents itself when an attacker passes a name for a target file, along with directory traversal sequences, to the affected application.

An attacker may leverage this issue to disclose arbitrary files on an affected computer. It was also reported that an attacker can supply NULL bytes with a target file name. This may aid in other attacks such as crashing the server.

2. MetaCart E-Shop ProductsByCategory.ASP Cross-Site Scripting ...

BugTraq ID: 13639

Remote: Yes

Date Published: May 16 2005

Relevant URL: <http://www.securityfocus.com/bid/13639>

Summary:

MetaCart e-Shop is prone to a cross-site scripting vulnerability. This issue is due to a failure in the

application to properly sanitize user-supplied input.

An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie-based authentication credentials as well as other attacks.

3. Mozilla Suite And Firefox Multiple Script Manager Security B...

BugTraq ID: 13641

Remote: Yes

Date Published: May 16 2005

Relevant URL: <http://www.securityfocus.com/bid/13641>

Summary:

Multiple issues exist in Mozilla Suite and Firefox. These issues allow attackers to bypass security checks in the script security manager.

Security checks in the script security manager are designed to prevent script injection vulnerabilities.

An attacker sending certain undisclosed JavaScript in 'view-source:', and 'jar:' pseudo protocol URIs, may bypass these security checks.

An undisclosed, nested URI, as well as a variant of BID 13216 are reportedly also able to bypass security checks.

These vulnerabilities allow remote attackers to execute script code with elevated privileges, leading to the installation and execution of malicious applications on an affected computer. Cross-site scripting, and other attacks are also likely possible.

The vendor has not provided enough information to determine how many specific instances of the issue were addressed, and has not clarified whether or not they have addressed a single general vulnerability or multiple specific vulnerabilities. This BID may be split into its separate issues as further information is disclosed.

Further details are scheduled to be released in the future. This BID will be updated at that time.

4. Mozilla Suite And Firefox DOM Property Overrides Code Execut...

BugTraq ID: 13645

Remote: Yes

Date Published: May 16 2005

Relevant URL: <http://www.securityfocus.com/bid/13645>

Summary:

Mozilla Suite and Mozilla Firefox are affected by a code execution vulnerability. This issue is due to a failure in the application to properly verify Document Object Model (DOM) property values.

An attacker may leverage this issue to execute arbitrary code with the privileges of the user that activated the vulnerable Web browser, ultimately facilitating a compromise of the affected computer.

This issue is reportedly a variant of BID 13233. Further details are scheduled to be released in the future, and this BID will be updated accordingly.

5. War Times Remote Game Server Denial Of Service Vulnerability

BugTraq ID: 13652

Remote: Yes

Date Published: May 17 2005

Relevant URL: <http://www.securityfocus.com/bid/13652>

Summary:

War Times is susceptible to a remote denial of service vulnerability. This issue is due to a failure of the application to properly bounds check user-supplied network data prior to copying it into a fixed-size memory buffer.

This vulnerability allows remote attackers to crash the game server, denying service to legitimate users.

Version 1.03, and prior are affected by this issue.

6. Fastream NETFile FTP/Web Server FTP Bounce Vulnerability

BugTraq ID: 13653

Remote: Yes

Date Published: May 17 2005

Relevant URL: <http://www.securityfocus.com/bid/13653>

Summary:

NETFile FTP/Web Server is affected by an FTP Bounce issue that can allow remote attackers to connect between the FTP server and an arbitrary port on another computer.

This could result in the proxying of arbitrary requests by a user through the system using the vulnerable FTP software.

This issue can allow attackers to bypass access controls and firewalls.

7. IgnitionServer Entry Deletion Access Validation Checking Vul...

BugTraq ID: 13654

Remote: Yes

Date Published: May 17 2005

Relevant URL: <http://www.securityfocus.com/bid/13654>

Summary:

ignitionServer is prone to an issue that allows hosts to delete access entries created by owners. This occurs because access validation is never performed when the host deletes the entry.

This issue was addressed in ignitionServer 0.3.6-P1.

8. IgnitionServer Locked Channel Protected Operator Lockout Vul...

BugTraq ID: 13656

Remote: Yes

Date Published: May 17 2005

Relevant URL: <http://www.securityfocus.com/bid/13656>

Summary:

ignitionServer is prone to an issue that can allow a user to lock a protected operator out of an IRC channel. This issue occurs because a validation check that should allow the protected operator to access the locked channel was not included in the application.

This issue was addressed in ignitionServer 0.3.6-P1.

9. Microsoft IPV6 TCPIP Loopback LAND Denial of Service Vulnera...

BugTraq ID: 13658

Remote: Yes

Date Published: May 17 2005

Relevant URL: <http://www.securityfocus.com/bid/13658>

Summary:

The Microsoft Windows IPV6 TCP/IP stack is prone to a "loopback" condition initiated by sending a TCP packet with the "SYN" flag set and the source address and port spoofed to equal the destination source and port.

When a packet of this type is handled, an infinite loop is initiated and the affected system halts.

A remote attacker may exploit this issue to deny service for legitimate users.

This issue is reported to affect Microsoft Windows XP Service Pack 2, Windows 2003 Server Service Pack 1.

10. MySQL mysql_install_db Insecure Temporary File Creation Vuln...

BugTraq ID: 13660

Remote: No

Date Published: May 17 2005

Relevant URL: <http://www.securityfocus.com/bid/13660>

Summary:

MySQL is reportedly affected by a vulnerability that can allow local attackers to gain unauthorized access to the database or gain elevated privileges. This issue results from a design error due to the creation of temporary files in an insecure manner.

The vulnerability affects the 'mysql_install_db' script.

Due to the nature of the script it may be possible to create database accounts or gain elevated privileges.

MySQL versions prior to 4.0.12 and MySQL 5.x releases 5.0.4 and prior versions are reported to be affected.

11. Microsoft HTML Help Workshop HHC.EXE HHA.DLL HHC Path Memory...

BugTraq ID: 13668

Remote: Yes

Date Published: May 17 2005

Relevant URL: <http://www.securityfocus.com/bid/13668>

Summary:

The Microsoft HTML Help Workshop compiler tool, 'hhc.exe', is prone to a memory corruption vulnerability.

Immediate consequences of exploitation of this issue result in an application crash; this would not be considered a vulnerability. However, it may be possible to subtly manipulate the contents of the affected registers so that an exploitable code path is reached. This has not been confirmed.

This BID will be updated or retired when further investigation of this issue is completed.

12. Avast! Antivirus Unspecified Scan Evasion Vulnerability

BugTraq ID: 13671

Remote: Yes

Date Published: May 18 2005

Relevant URL: <http://www.securityfocus.com/bid/13671>

Summary:

Avast! Antivirus is prone to an unspecified scan evasion vulnerability. Reports indicate that the issue manifests because the software fails to properly handle certain unspecified types of files.

This issue could result in a malicious executable file bypassing detection and being executed, based on a false sense of trust, by a recipient.

No further details are available in regard to this issue. However, this BID will be updated as soon as further information is made public.

13. Multiple Vendor TCP Timestamp PAWS Remote Denial Of Service ...

BugTraq ID: 13676

Remote: Yes

Date Published: May 18 2005

Relevant URL: <http://www.securityfocus.com/bid/13676>

Summary:

A denial of service vulnerability exists for the TCP RFC 1323. The issue exists in the Protection Against Wrapped Sequence Numbers (PAWS) technique that was included to increase overall TCP performance.

When TCP 'timestamps' are enabled, both hosts at the endpoints of a TCP connection employ internal clocks to mark TCP headers with a 'time stamp' value.

When TCP PAWS is configured to employ timestamp values, this functionality exposes TCP PAWS implementations to a denial of service vulnerability.

The issue manifests if an attacker transmits a sufficient TCP PAWS packet to a vulnerable computer. A large value is set by the attacker as the packet timestamp. When the target computer processes this packet, the internal timer is updated to the large attacker supplied value. This causes all other valid packets that are received subsequent to an attack to be dropped as they are deemed to be too old, or invalid. This type of attack will effectively deny service for a target connection.

14. Microsoft Outlook HTML Email URI Spoofing Vulnerability

BugTraq ID: 13677

Remote: Yes

Date Published: May 18 2005

Relevant URL: <http://www.securityfocus.com/bid/13677>

Summary:

Microsoft Outlook is reportedly affected by a URI spoofing vulnerability. This issue allows a URI in an email message to be misrepresented.

An attacker can trick users into following links to untrusted sites, which can lead to various attacks.

All versions of Microsoft Outlook are reportedly vulnerable to this issue.

It appeared that this issue allowed for address bar spoofing in Microsoft Outlook, however, further analysis has revealed that this is not correct. This functionality is included in HTML. This BID is being retired.

15. Groove Networks Groove Virtual Office File Extension Obfusca...

BugTraq ID: 13682

Remote: Yes

Date Published: May 19 2005

Relevant URL: <http://www.securityfocus.com/bid/13682>

Summary:

Groove Virtual Office is affected by a vulnerability that allows remote attackers to obfuscate file extensions of potentially malicious files.

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #242

The file extension of a specially crafted file may be obfuscated in a manner that creates a false sense of security for a user.

The user may be inclined to open a malicious file that could lead to arbitrary code execution. This may allow an attacker to gain unauthorized access to a computer in the context of the vulnerable user.

16. Groove Networks Groove Virtual Office SharePoint Lists Arbit...

BugTraq ID: 13684

Remote: Yes

Date Published: May 19 2005

Relevant URL: <http://www.securityfocus.com/bid/13684>

Summary:

Groove Virtual Office is affected by an arbitrary script injection vulnerability.

User-supplied data is not properly sanitized from SharePoint lists and is copied into Groove Mobile Workspace. This can allow an attacker to inject and execute script code in the context of the application, which can lead to various attacks.

17. Groove Networks Groove Virtual Office COM Object Security By...

BugTraq ID: 13685

Remote: Yes

Date Published: May 19 2005

Relevant URL: <http://www.securityfocus.com/bid/13685>

Summary:

Groove Virtual Office is prone to a security bypass vulnerability with regards to COM objects. Due to a failure in the application an attacker may be able to bypass the security restrictions on COM objects and execute arbitrary code.

This issue has been addressed in Groove Virtual Office 3.1 build 2338, 3.1a build 2364, and Groove Workspace Version 2.5n build 1871.

18. Microsoft Word MCW File Handler Buffer Overflow Vulnerabilit...

BugTraq ID: 13687

Remote: Yes

Date Published: May 19 2005

Relevant URL: <http://www.securityfocus.com/bid/13687>

Summary:

Microsoft Word is prone to a buffer overflow vulnerability. The issue manifests when a '.mcw' (MacWrite II/MS Word for Macintosh) file is processed.

It is conjectured that this issue may be exploited to execute arbitrary code in the context of a user that processes a malicious file with the affected software.

19. Groove Networks Groove Mobile Workspace SharePoint Lists Arb...

BugTraq ID: 13688

Remote: Yes

Date Published: May 19 2005

Relevant URL: <http://www.securityfocus.com/bid/13688>

Summary:

Groove Virtual Office is affected by an arbitrary script injection vulnerability.

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #242

User-supplied data is not properly sanitized from SharePoint lists and is copied into Groove Mobile Workspace. This can allow an attacker to inject and execute script code in the context of the application, which can lead to various attacks.

20. NetWin SurgeMail Multiple Unspecified Input Validation Vulne...

BugTraq ID: 13689

Remote: Yes

Date Published: May 19 2005

Relevant URL: <http://www.securityfocus.com/bid/13689>

Summary:

Multiple unspecified vulnerabilities affect SurgeMail. Reportedly, these issues are due to a failure of the application to properly sanitize user-supplied input prior to employing it in critical locations including dynamic content. A successful attack may allow attackers to execute arbitrary HTML and script code in a user's browser.

SurgeMail 3.0c2 is reported to be affected by these issues. Other versions may be vulnerable as well.

Due to a lack of details, further information cannot be provided at the moment. This BID will be updated when more details are available.

21. ImageMagick And GraphicsMagick XWD Decoder Denial Of Service...

BugTraq ID: 13705

Remote: Yes

Date Published: May 21 2005

Relevant URL: <http://www.securityfocus.com/bid/13705>

Summary:

A remote, client-side denial of service vulnerability affects ImageMagick and GraphicsMagick. This issue is due to a failure of the application to handle malformed XWD image files.

A remote attacker may leverage this issue to cause the affected application to enter into an infinite loop condition, consuming CPU resources on the affected computer, denying service to legitimate users.

III. MICROSOFT FOCUS LIST SUMMARY

1. Encrypting remote files with EFS (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/398846>

2. SecurityFocus Microsoft Newsletter #241 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/398515>

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. tcpdump for Windows 1.0 beta

By: microOLAP Technologies

Relevant URL: <http://microolap.com/products/network/tcpdump/>

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

Summary:

MicroOLAP TCPDUMP for Windows accurately reproduces all features of the original tcpdump by LBNL's Network Research Group, developed for the UNIX

systems. Since MicroOLAP TCPDUMP for Windows is compiled with the Packet Sniffer SDK, it has the following advantages:

- does not require any third-party preinstalled drivers;
- works from the single 300K .EXE file;
- supports 1Gbit networks.

2. Assimilator 1.0.0

By: Black List Software

Relevant URL: <http://hackinoutthebox.com/sub5.index.php>

Platforms: Windows XP

Summary:

Assimilation is the result of assimilating something which is dissimilated. In other words, assimilation is the result of making two dissimilar things similar. Assimilation can be based on a baseline. A baseline is a standard or protocol which is in place for the sake of governing events. In the case of Assimilator v1.0.0, our baseline is a replication of the good processes which run locally on our computers.

3. Cenzic Hailstorm 2.0

By: Cenzic, Inc.

Relevant URL: http://www.cenzic.com/prod_application_security.html

Platforms: Windows XP

Summary:

Cenzic Hailstorm automates penetration testing for your web applications. Cenzic Hailstorm provides various groups ? Information Security, QA, and Developers ? throughout the enterprise an ability to test applications for security vulnerabilities, for enforcement of internal security policies, and for regulatory compliance-crafted policy library to address new and unique vulnerabilities.

4. VForce 2.1.008

By: Virtual Forge

Relevant URL: http://solutions.virtualforge.net/sol_download_en.php

Platforms: Windows NT, Windows XP

Summary:

V-Force is an instrument with whose help attacks on web server or applications can be simulated and the results logged and analyzed.

5. Multiple Interface Watcher 1.0

By: Carsten Schmidt

Relevant URL: <http://software.ccschmidt.de/#MIW>

Platforms: Windows 2000, Windows NT, Windows XP

Summary:

Multiple Interface Watcher is a graph utility that shows the utilisation of up to 10 different interfaces. The data is requested from the devices using SNMP. MIW is an advanced development of Interface Traffic Indicator that focuses more on the utilization overview of many interfaces than on much information of one interface.

6. LC 5 5

By: @stake

Relevant URL: <http://www.atstake.com/products/lc/>

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #242

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

Summary:

LC 5 is the latest version of L0phtCrack, the award-winning password auditing and recovery application used by thousands of companies worldwide.

Using multiple assessment methods, LC 5 reduces security risk by helping administrators to:

- * Identify and remediate security vulnerabilities that result from the use of weak or easily guessed passwords
- * Recover Windows and Unix account passwords to access user and administrator accounts whose passwords are lost or to streamline migration of users to another authentication system
- * Rapidly process accounts using pre-computed password tables* that contain trillions of passwords

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
