

SecurityFocus Microsoft Newsletter #232

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-03/0123.html>

From: Marc Fossi (mfossi_at_securityfocus.com)

Date: 03/16/05

Date: Wed, 16 Mar 2005 09:43:46 -0700 (MST)

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

SecurityFocus Microsoft Newsletter #232

This Issue is Sponsored By: Black Hat

Make plans now to attend the Black Hat Briefings & Training Europe, March 29–April 1 in Amsterdam, the world's premier technical security event. Featuring 30 speakers in four tracks, 10 training sessions, with 250 delegates from 20 nations attending. Learn about the technical security market drivers in the European market. Visit www.blackhat.com for information or to register.

http://www.securityfocus.com/sponsor/BlackHat_ms-secnews_050315

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. Infection Vectors
2. A Method for Forensic Previews
3. Windows Firewalls Lacking

II. MICROSOFT VULNERABILITY SUMMARY

1. PHPBB Session.PHP Autologin User_Level Privilege Escalation ...
2. Gene6 FTP Server Remote Default Install Code Execution Vulne...
3. SafeNet Sentinel License Manager Remote Buffer Overflow Vuln...
4. Hosting Controller Multiple Information Disclosure Vulnerabi...
5. Yahoo! Messenger Offline Mode Status Remote Buffer Overflow ...
6. YaBB Remote UsersRecentPosts Cross-Site Scripting Vulnerabil...
7. Drupal Unspecified Cross-Site Scripting Vulnerability

8. PHP Arena PAFileDB Multiple Remote Cross Site Scripting Vuln...
9. Microsoft Exchange Server Mail Box Sub Folder Denial Of Serv...
10. Microsoft Internet Explorer MSHTML.DLL CSS Handling Remote B...
11. Multiple Vendor Antivirus Products Malformed ZIP Attachment ...
12. MySQL AB MySQL Multiple Remote Vulnerabilities

III. MICROSOFT FOCUS LIST SUMMARY

1. Limitlogin v1.0 released from MS (Thread)
2. Question on IIS servers and reverse lookup ... found... (Thread)
3. Basic question (Thread)
4. Folder Encryption (Thread)
5. Question on IIS servers and reverse lookup (Thread)
6. SecurityFocus Microsoft Newsletter #231 (Thread)
7. Disabling USB mass storage (Thread)
8. SID Manipulation Issue – Cross Domain Security Vulne... (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. Healthmonitor 2.1
2. Kr4ck3r 1.0.0
3. WinArpSpoof 0.5.3
4. SafeLogon 2.0
5. SafeSystem 1.5
6. SQL column finder 0.1

VI. UNSUBSCRIBE INSTRUCTIONS

VII. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Infection Vectors

By Kelly Martin

It's time to pick your favorite virus.

<http://www.securityfocus.com/columnists/306>

2. A Method for Forensic Previews

By Timothy E. Wright

This article explains the forensic preview process, whereby a production machine is left as undisturbed as possible while it is evaluated for potential intrusion and compromise.

<http://www.securityfocus.com/infocus/1825>

3. Windows Firewalls Lacking

By Mark Burnett

For something as simple as a firewall for Windows servers, a good solution just doesn't exist.

<http://www.securityfocus.com/columnists/307>

II. MICROSOFT VULNERABILITY SUMMARY

1. PHPBB Session.PHP Autologin User_Level Privilege Escalation ...

BugTraq ID: 12736

Remote: Yes

Date Published: Mar 07 2005

Relevant URL: <http://www.securityfocus.com/bid/12736>

Summary:

phpBB is reported prone to a privilege escalation vulnerability. The issue is reported to exist when an autologin fails.

A remote attacker may potentially exploit this vulnerability to gain access to parts of the affected website that should only be visible to a website administrator.

Information harvested through exploitation of this vulnerability may be employed to aid in further attacks against the affected site.

This vulnerability is reported to affect phpBB versions up to up to 2.0.13.

2. Gene6 FTP Server Remote Default Install Code Execution Vulne...

BugTraq ID: 12739

Remote: Yes

Date Published: Mar 07 2005

Relevant URL: <http://www.securityfocus.com/bid/12739>

Summary:

Reportedly a remote code execution vulnerability affects Gene6 FTP Server. This issue is due to a configuration error that fails to secure critical functionality from default users.

An attacker that can authenticate to the affected FTP server can execute arbitrary code with SYSTEM privileges; this will facilitate privilege escalation.

3. SafeNet Sentinel License Manager Remote Buffer Overflow Vuln...

BugTraq ID: 12742

Remote: Yes

Date Published: Mar 07 2005

Relevant URL: <http://www.securityfocus.com/bid/12742>

Summary:

A remote buffer overflow vulnerability affects SafeNet Sentinel License Manager. This issue is due to a failure of the application to securely copy network-derived data into finite process buffers.

An attacker may leverage this issue to execute arbitrary code with SYSTEM privileges.

4. Hosting Controller Multiple Information Disclosure Vulnerabi...

BugTraq ID: 12748

Remote: Yes

Date Published: Mar 07 2005

Relevant URL: <http://www.securityfocus.com/bid/12748>

Summary:

Hosting Controller is reported prone to multiple information disclosure vulnerabilities. These issues can allow an attacker to disclose sensitive information, which may be used to carry out further attacks against a computer.

An attacker can access a sensitive file to enumerate domain names of all hosted domains.

Another issue affecting the application may allow remote users to disclose an administrator's email address.

These issues are reported to affect Hosting Controller 6.1 Hotfix 1.7. Other versions are likely to be affected as well.

5. Yahoo! Messenger Offline Mode Status Remote Buffer Overflow ...

BugTraq ID: 12750

Remote: Yes

Date Published: Mar 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12750>

Summary:

It has been reported that a remote buffer overflow vulnerability affects Yahoo! Messenger. This issue is due to a failure of the application to securely copy user-supplied input into finite process buffers.

It is likely that the attacker must be in the contact list of an unsuspecting user to exploit this issue. It should be noted that the details surrounding this issue are not clear; this BID will be updated as more details are released.

An attacker may leverage this issue to execute arbitrary code in the context of an unsuspecting user running a vulnerable version of the affected application.

6. YaBB Remote UsersRecentPosts Cross-Site Scripting Vulnerabil...

BugTraq ID: 12756

Remote: Yes

Date Published: Mar 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12756>

Summary:

A remote cross-site scripting vulnerability affects YaBB. This issue is due to a failure of the application to properly sanitize user-supplied input prior to including it in dynamically generated Web content.

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.

7. Drupal Unspecified Cross-Site Scripting Vulnerability

BugTraq ID: 12757

Remote: Yes

Date Published: Mar 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12757>

Summary:

An unspecified remote cross-site scripting vulnerability affects Drupal. This issue is due to a failure of the application to properly sanitize user-supplied input prior to using it in dynamically generated Web page content.

An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user.

This vulnerability is reported to affect Drupal versions prior to version 4.5.2.

8. PHP Arena PaFileDB Multiple Remote Cross Site Scripting Vuln...

BugTraq ID: 12758

Remote: Yes

Date Published: Mar 08 2005

Relevant URL: <http://www.securityfocus.com/bid/12758>

Summary:

Multiple remote cross-site scripting vulnerabilities affect PHP Arena PaFileDB. These issues are due to a failure of the application to properly sanitize user-supplied input prior to including it in dynamically generated Web content.

An attacker may leverage these issues 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.

9. Microsoft Exchange Server Mail Box Sub Folder Denial Of Serv...

BugTraq ID: 12764

Remote: Yes

Date Published: Mar 09 2005

Relevant URL: <http://www.securityfocus.com/bid/12764>

Summary:

A denial of service vulnerability affects Microsoft Exchange Server. This issue is due to the application failing to efficiently handle the manipulation of specially crafted folders.

An attacker may leverage this issue to cause the Microsoft Exchange Information Store service to stop responding, denying service to legitimate users.

10. Microsoft Internet Explorer MSHTML.DLL CSS Handling Remote B...

BugTraq ID: 12765

Remote: Yes

Date Published: Mar 09 2005

Relevant URL: <http://www.securityfocus.com/bid/12765>

Summary:

Microsoft Internet Explorer is reported prone to a remote buffer overflow vulnerability.

This issue presents itself when the application handles a malformed CSS file.

A typical attack would involve the attacker creating a Web site that includes the malicious CSS file. The attacker may then entice a vulnerable user to visit the site. If successful, this attack may result in granting the attacker unauthorized access to the affected computer in the context of the user running Internet Explorer.

This issue may be related to BID 10816 (Microsoft Internet Explorer Style Tag Comment Memory Corruption Vulnerability) and may have been fixed by Microsoft Security Bulletin MS04-038. This is not confirmed at the moment. This BID will be updated when further technical analysis is complete.

11. Multiple Vendor Antivirus Products Malformed ZIP Attachment ...

BugTraq ID: 12771

Remote: Yes

Date Published: Mar 10 2005

Relevant URL: <http://www.securityfocus.com/bid/12771>

Summary:

Multiple antivirus products from various vendors are reported prone to a vulnerability that may allow potentially malformed ZIP archives to bypass detection.

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #232

This issue arises when an affected application processes a ZIP archive with an invalid CRC-32 checksum. It should be noted that affected software may possibly detect a malicious file in the archive when it is decompressed or scanned manually.

The discoverer of this vulnerability has reported that this issue affects H+BEDV AntiVir, AVG Anti-Virus, Sybari Antigen for Microsoft Exchange, and products by McAfee, and BitDefender. Symantec products were not found to be vulnerable to the issue.

****Update:** Symantec believes that the impact of this issue is low. This is because an archive handler processing an archive that possesses a corrupt CRC-32 checksum will fail, reporting that the archive is corrupt. This would mean that a malicious file contained in such an archive would not be directly accessible to a target recipient user.

Alternatively, if the CRC-32 checksum is corrected manually by the recipient user and the file is extracted, it will likely be detected by client-side Anti-Virus solutions during the file extraction routine. This detection will likely occur before the malicious file is directly processed by the end user.

12. MySQL AB MySQL Multiple Remote Vulnerabilities

BugTraq ID: 12781

Remote: Yes

Date Published: Mar 11 2005

Relevant URL: <http://www.securityfocus.com/bid/12781>

Summary:

MySQL is reported prone to multiple vulnerabilities that can be exploited by a remote authenticated attacker. The following individual issues are reported:

MySQL is reported prone to an insecure temporary file creation vulnerability.

Reports indicate that an attacker that has 'CREATE TEMPORARY TABLE' privileges on an affected installation may leverage this vulnerability to corrupt files with the privileges of the MySQL process.

MySQL is reported prone to an input validation vulnerability that can be exploited by remote users that have INSERT and DELETE privileges on the 'mysql' administrative database.

Reports indicate that this issue may be leveraged to load and execute a malicious library in the context of the MySQL process.

Finally, MySQL is reported prone to a remote arbitrary code execution vulnerability. It is reported that the vulnerability may be triggered by employing the 'CREATE FUNCTION' statement to manipulate functions in order to control sensitive data structures.

This issue may be exploited to execute arbitrary code in the context of the database process.

These issues are reported to exist in MySQL versions prior to MySQL 4.0.24 and 4.1.10a.

III. MICROSOFT FOCUS LIST SUMMARY

1. Limitlogin v1.0 released from MS (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/393187>

2. Question on IIS servers and reverse lookup ... found... (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/393102>

3. Basic question (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/393101>

4. Folder Encryption (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/393095>

5. Question on IIS servers and reverse lookup (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/392937>

6. SecurityFocus Microsoft Newsletter #231 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/392708>

7. Disabling USB mass storage (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/392707>

8. SID Manipulation Issue – Cross Domain Security Vulne... (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/392618>

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. Healthmonitor 2.1

By: Vittorio Pavesi

Relevant URL: <http://healthmonitor.sourceforge.net>

Platforms: Windows 2000, Windows NT, Windows XP

Summary:

HealthMonitor is a free powerful and featureful monitoring tool for Windows.

It works as a Windows Service and check system status (event viewer, disk free space, services status, performance....) and notify the administration by E-Mail, SMS and by NET SEND; a database logging feature is also available. It is under constant development, and releases are usually frequent. The latest news regarding HealthMonitor can be found on Sourceforge.

2. Kr4ck3r 1.0.0

By: Black List Software

Relevant URL: <http://hackinoutthebox.com/sub4.index.php>

Platforms: Windows XP

Summary:

This is the ultimate MD5 cracker having both a built-in brute-force and dictionary attack functionality.

3. WinArpSpoof 0.5.3

By: Gordon Ahn

Relevant URL: <http://www.nextsecurity.net/downloads/winarpspoof/WinArpSpoof.zip>

Platforms: Windows 2000, Windows NT, Windows XP

Summary:

Windows ARP Spoofer (WinArpSpoof) is a program that can scan the computers including network devices and can spoof their ARP tables on local area network and can act as a router while pulling all packets on LAN. In addition, traffic information through this program is measured.

4. 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

5. 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

6. 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

VI. UNSUBSCRIBE INSTRUCTIONS

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #232

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

This Issue is Sponsored By: Black Hat

Make plans now to attend the Black Hat Briefings & Training Europe, March 29–April 1 in Amsterdam, the world's premier technical security event. Featuring 30 speakers in four tracks, 10 training sessions, with 250 delegates from 20 nations attending. Learn about the technical security market drivers in the European market. Visit www.blackhat.com for information or to register.

http://www.securityfocus.com/sponsor/BlackHat_ms-secnews_050315

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
