

SecurityFocus Microsoft Newsletter #138

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-05/0087.html>

From: Marc Fossi (*mfossi_at_securityfocus.com*)

Date: 05/27/03

Date: Tue, 27 May 2003 09:33:49 -0600 (MDT)

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

SecurityFocus Microsoft Newsletter #138

This Issue is Sponsored By: SpiDynamics

ALERT: Top 10 Web Application Attack Techniques and Methods to Combat them
Learn why 70% of today's successful hacks involve Web Application attacks such as: SQL Injection, XSS, Cookie Manipulation, and Parameter Manipulation.

All undetectable by Firewalls and IDS!

Download *FREE* white paper from SPI Dynamics for a complete guide to protection!

Visit us at: <http://www.spidynamics.com/mktg/webappsecurity102>

I. FRONT AND CENTER

1. Passive Network Traffic Analysis: Understanding a Network...
2. Conducting a Security Audit: An Introductory Overview
3. Cyber Insurance Between the Lines

II. MICROSOFT VULNERABILITY SUMMARY

1. Microsoft ISA Server Error Page Cross-Site Scripting...
2. PHP-Nuke Statistics Module Mainfile.PHP Cross-Site...
3. PHP-Banner Exchange Path Disclosure Vulnerability
4. Compaq Management Agents Remote Authentication Bypass...
5. Nessus LibNASL Arbitrary Code Execution Vulnerability
6. EServ Directory Indexing Vulnerability
7. EServ Unauthorized Proxy Access Vulnerability
8. Snort Spoofed Packet TCP State Evasion Vulnerability
9. Working Resources BadBlue Unauthorized HTS Access Vulnerability
11. BZFlag Reconnect Denial Of Service Vulnerability
12. Platform Load Sharing Facility LSF_ENVDIR Local Command...
13. IISProtect Authentication Bypass Vulnerability
14. PHPNuke Remote Main Modules Multiple SQL Injection...
15. Blackmoon FTP Server Username Information Disclosure...

17. Apple QuickTime/Darwin Streaming Server QTSSReflector Module...
18. Apple QuickTime/Darwin Streaming MP3Broadcaster ID3 Tag...
19. Microsoft Internet Connection Firewall IPv6 Traffic Blocking...
20. Microsoft Netmeeting CALLTO URL Buffer Overflow Vulnerability
21. Microsoft Windows Media Player Automatic File Download and...
22. Demarc PureSecure Plaintext Password Vulnerability
23. Magic Winmail Server USER POP3 Command Format String...

III. MICROSOFT FOCUS LIST SUMMARY

1. Windows 2003 Server – MS Rulez? (Thread)
2. Updated URLScan Security Tool Released (Thread)
3. Netreg for Windows (Thread)
4. Article Announcement: Passive Network Traffic Analysis:...
5. Administrivia: Sobig/Mankx/Palyh (Thread)
6. SecurityFocus Microsoft Newsletter #137 (Thread)
7. Article Announcement: "Relax, It Was a Honeypot" (Thread)
8. Article Announcement: Malware Myths and Misinformation, Part...

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. CryptoGram Secure Login
2. Tricryption Engine
3. neuSECURE

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. WinCrypt v2.0
2. Darik's Boot and Nuke v2003052000(Beta)
3. incident.pl v2.6

VI. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Passive Network Traffic Analysis: Understanding a Network Through Passive Monitoring
By Kevin Timm

This article will offer a brief overview of passive network monitoring, which can offer a thorough understanding of the network's topology: what services are available, what operating systems are in use, and what vulnerabilities may be exposed on the network.

<http://www.securityfocus.com/infocus/1696>

2. Conducting a Security Audit: An Introductory Overview
By Bill Hayes

This article will offer a brief overview of security audits: what they are, why they are important, and how they are conducted.

<http://www.securityfocus.com/infocus/1697>

3. Cyber Insurance Between the Lines
By Mark Rasch

Your company may already have insurance against computer attacks and electronic sabotage, without even knowing it.

<http://www.securityfocus.com/columnists/163>

II. BUGTRAQ SUMMARY

1. Microsoft ISA Server Error Page Cross-Site Scripting Vulnerability

BugTraq ID: 7623

Remote: Yes

Date Published: May 17 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7623>

Summary:

Microsoft ISA (Internet Security and Acceleration) Server is an application firewall that also provides intrusion detection capabilities.

A cross-site scripting vulnerability has been reported for Microsoft ISA Server. The vulnerability exists due to insufficient sanitization of certain HTTP header fields. Specifically, ISA Server does not properly sanitize malicious HTML code from the 'Via:' HTTP header.

The attacker may be required to create a malicious link to a site and then entice web users to visit the link.

Successful exploitation could permit a malicious attacker to cause the execution of hostile HTML and script code in the web client of a user who visits the malicious link. This would occur in the security context of the site.

Exploitation could allow for attacks that steal cookie-based authentication credentials. Other attacks will also be possible.

2. PHP-Nuke Statistics Module Mainfile.PHP Cross-Site Scripting Vulnerability

BugTraq ID: 7624

Remote: Yes

Date Published: May 17 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7624>

Summary:

PHP-Nuke is a web-based portal system. Implemented in PHP, it is available for a range of systems, including Unix, Linux, and Microsoft Windows.

The PHP-Nuke 'mainfile.php' script does not sufficiently sanitize data supplied via URI parameters, making it prone to cross-site scripting attacks. In particular, the 'year' URI parameter is not properly sanitized of HTML tags. This could allow for execution of hostile HTML and script code in the web client of a user who visits a web page that contains the malicious code. This would occur in the security context of the site

hosting the software.

Exploitation could allow for theft of cookie-based authentication credentials. Other attacks are also possible.

3. PHP-Banner Exchange Path Disclosure Vulnerability

BugTraq ID: 7636

Remote: Yes

Date Published: May 20 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7636>

Summary:

PHP-Banner Exchange is banner management software. It is written in PHP and available for a number of operating systems including Microsoft Windows and Unix and Linux variants.

PHP-Banner Exchange is prone to a path disclosure vulnerability. Requesting the directory for the software will cause an error message to be displayed with contains path information.

PHP-Banner Exchange can be used as a module for PHP-Nuke.

Exploitation may be dependant on web server and PHP configuration.

This type of information may aid an attacker in mapping out the filesystem for further attacks against the host.

4. Compaq Management Agents Remote Authentication Bypass Vulnerability

BugTraq ID: 7648

Remote: Yes

Date Published: May 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7648>

Summary:

Compaq Management Agents is a web-based interface designed to monitor various system device parameters. It is available for a variety of operating systems including Unix, GNU/Linux, and Microsoft Windows.

A vulnerability has been reported for Compaq Management Agents (CMA). The problem is said to present itself when anonymous access has been enabled. Supposedly, if the administrator password has been changed from the default, an unauthorized remote user may gain administrative access. This can be accomplished by placing 'administrator' in all fields at the password screen.

Successful exploitation of this issue will allow an attacker to gain administrative access to the CMA interface. This may result in the tampering of sensitive system device settings or possibly other attacks.

This vulnerability has been reported to affect Compaq Management Agents 4.36 and Insight Manager Version 5.0.

5. Nessus LibNASL Arbitrary Code Execution Vulnerability

BugTraq ID: 7664

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7664>

Summary:

Nessus is a vulnerability scanning utility available for the Unix and Microsoft Windows operating systems. libnasl is a library used by Nessus to process NASL scripts.

Nessus has reported that various flaws have been discovered in the libnasl library. Amongst other functions, scanner_add_port(), insstr() and ftp_log_in() fail to sufficiently handle malformed parameters and may allow a script to break out of the established sandbox environment. As a result, it may be possible for a malicious Nessus plugin to execute arbitrary system commands with the privileges of Nessus the application, possibly root.

It should be noted that this malicious script must be a legitimate plugin which has been uploaded to the Nessus server. Furthermore, the affected Nessus application must have enabled the 'plugins_upload' option which is disabled by default.

The precise details regarding this vulnerability are currently unknown. This BID will be updated as further information becomes available.

Although unconfirmed, these vulnerabilities may be exploited to execute arbitrary attacker-supplied code.

This issue affects Nessus version 2.05 and earlier.

6. EServ Directory Indexing Vulnerability

BugTraq ID: 7669

Remote: Yes

Date Published: May 23 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7669>

Summary:

EServ is a combination Mail, News, Web, FTP and Proxy Server for Microsoft Windows systems.

EServ does not sufficiently prevent web users from being able to view directory indexes. This is reported to be an issue even when a directory has an index file. This may result in disclosure of sensitive information which may be useful in further attacks against the system.

7. EServ Unauthorized Proxy Access Vulnerability

BugTraq ID: 7670

Remote: Yes

Date Published: May 23 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7670>

Summary:

EServ is a combination Mail, News, Web, FTP and Proxy Server for Microsoft Windows systems.

EServ is prone to a vulnerability that may allow it to be used as a proxy by unauthorized remote users. This can occur even if a proxy authentication is required or the proxy service is disabled. Users can proxy request through port 80 if the proxy service is disabled. It has also been reported that the FTP proxy may also be abused in a similar manner.

8. Snort Spoofed Packet TCP State Evasion Vulnerability

BugTraq ID: 7635

Remote: Yes

Date Published: May 20 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7635>

Summary:

Snort is a freely available, open source intrusion detection system. It is available for Unix, Linux, and Microsoft Windows platforms.

A vulnerability has been reported within the spp_stream4.c source file. The problem is said to occur while maintaining the state of an established session.

Specifically, Snort is said to call UpdateState before verifying the legitimacy of a packet received from a client partaking in a legitimate session. As a result, it may be possible to corrupt stateful inspection carried out by Snort.

This issue can be triggered by forging a packet to a server containing the legitimate client source IP and port. When encountered by Snort, the state of the session is updated before verifying that the packet is a legitimate part of the established session. However when the packet is received by the server, due to invalid sequence and acknowledgement data, the packet will be dropped.

An attacker could exploit this vulnerability to trigger a situation under which legitimate session traffic transmitted would no longer be detected by Snort.

This vulnerability has been reported to affected Snort 2.0.0rc2, however other versions may also be affected.

It should be noted that this is a theoretical issue and has not yet been officially confirmed.

9. Working Resources BadBlue Unauthorized HTS Access Vulnerability
BugTraq ID: 7638

Remote: Yes

Date Published: May 20 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7638>

Summary:

BadBlue is a P2P file sharing application distributed by Working Resources. It is available for Microsoft Windows operating systems.

BadBlue is prone to a vulnerability that could allow remote attackers to gain unauthorized access to administrative functions. BadBlue includes a server-side scripting language which uses '.htx' and '.hts' files. The '.hts' extension represents files that are only intended to be requested and executed by the local host.

It is possible to bypass BadBlue security checks when '.hts' files are requested by a remote user. BadBlue restricts access to non-HTML files by replacing the first two letters in the file extension of a requested resource with 'ht'. If the third character of a file extension is 's', then it is possible to trick BadBlue into serving a non-HTML file with an extension of '.hts'. This will bypass other security checks which would normally prevent BadBlue from serving these files to remote users.

Exploitation could result in unauthorized access to administrative functions provided in '.hts' files.

10. Blackmoon FTP Server Plaintext User Password Weakness

BugTraq ID: 7646

Remote: No

Date Published: May 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7646>

Summary:

Blackmoon FTP Server is an FTP Server for Microsoft Windows operating systems.

Blackmoon FTP Server stores authentication credentials for the FTP service on the local system in plaintext. These credentials are stored in the 'blackmoon.mdb' file in the program directory. Local users with access to this file may gain unauthorized access to the server as a result.

Exposure of authentication credentials may also lead to compromise of other services/resources if the same credentials are commonly used.

It should be noted that although this weakness was reported to affect Blackmoon FTP server version 2.6, previous versions might also be affected.

11. BZFlag Reconnect Denial Of Service Vulnerability

BugTraq ID: 7649

Remote: Yes

Date Published: May 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7649>

Summary:

BZFlag is a multi-player action game. It is available for a number of operating systems, including Microsoft Windows and Unix/Linux variants.

BZFlag is prone to a denial of service vulnerability. Users that have established a session with BZFlag may cause a denial of service by reconnecting and flooding BZFlag ports with excessive amounts of data. This may reportedly cause a server crash or a memory leak that could exhaust available resources. Though unconfirmed, exploitation could result in memory corruption, which may allow for execution of malicious code.

This issue was reported in BZFlag 1.7g0. Other versions are also likely affected.

12. Platform Load Sharing Facility LSF_ENVDIR Local Command Execution Vulnerability

BugTraq ID: 7655

Remote: No

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7655>

Summary:

Load Sharing Facility is a high availability and load balancing software package distributed and maintained by Platform. It is available for Unix, Linux, and Microsoft Windows.

A problem in the software for the Unix and Linux platform may make it possible for a local user to gain unauthorized privileges.

It has been reported that Load Sharing Facility (LSF) does not properly handle input in environment variables. Because of this, an attacker may be able to gain escalated privileges on a vulnerable system.

The problem is in the handling of environment variables. When the lsadmin program is executed, shortly after starting execution it calls the lim program. The path to this program is specified in the configuration file. However, it is possible to change the location that will be checked for this program by altering the LSF_ENVDIR environment variable to force lsadmin to look for the lim program in a different location. By doing so,

it is possible to create a malicious copy of the lim program which would be executed with the privileges of the lsadmin program. The lsadmin program is typically installed with elevated privileges.

13. IISProtect Authentication Bypass Vulnerability

BugTraq ID: 7661

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7661>

Summary:

iisProtect is a security product for Microsoft Windows that provides authentication based access control to protect web resources.

A vulnerability has been reported that may allow for iisProtect authentication to be circumvented by web users. It is possible to bypass authentication to gain access to web resources by submitting a request which URL encoded character representations. iisProtect fails to recognize these character representations, but the underlying IIS server will interpret them and serve the resource that is requested.

Remote attackers may exploit this issue to gain access to sensitive web resources, which could allow for other attacks which compromise web resources.

14. PHPNuke Remote Main Modules Multiple SQL Injection Vulnerabilities

BugTraq ID: 7631

Remote: Yes

Date Published: May 20 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7631>

Summary:

PHPNuke is a freely available, open source web content management system. It is maintained by Francisco Burzi, and available for the Unix, Linux, and Microsoft Operating Systems.

Multiple input checking problems may make it possible for remote users to pass malicious data to the database.

It has been reported that multiple problems exist in the PHPNuke main modules. SQL injection issues exist in the Sections, Avantgo, Surveys, Downloads, Reviews, and Web_Links modules. This could allow an attacker pass malicious SQL code to the database. It should be noted that multiple path disclosure issues also exist.

Each of these modules does not properly handle the backtick character at precise locations in queries. Because of this, it is possible to create a custom command that will be executed with the privileges of the PHPNuke application.

15. Blackmoon FTP Server Username Information Disclosure Vulnerability

BugTraq ID: 7647

Remote: Yes

Date Published: May 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7647>

Summary:

Blackmoon FTP Server is an FTP Server for Microsoft Windows operating systems.

It has been reported that Blackmoon FTP Server is prone to an information disclosure weakness.

The problem exists in the way the FTP server handles the authentication procedure. Specifically the FTP server returns a '530–Account does not exist.' error message to the console, if the username supplied is invalid, before disconnecting the user. An attacker may exploit this weakness to enumerate valid usernames.

It should be noted that although this weakness was reported to affect Blackmoon FTP server version 2.6, previous versions might also be affected.

16. ShareMailPro Username Identification Weakness

BugTraq ID: 7658

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7658>

Summary:

ShareMailPro is an e–mail server solution designed for use with Microsoft Windows systems.

A weakness has been reported in ShareMailPro that may reveal the existence of usernames to remote attackers.

This weakness is due to the fact that ShareMailPro responds with different messages depending on whether a given username exists or not.

If an attacker connects with a non–existent username, the following message is displayed:

–ERR sorry , no such mailbox

An attacker may be able to use this information to launch further intelligent attacks against the server or to launch a brute force password attack against a known user name.

This vulnerability was reported for ShareMailPro 3.6.1.

17. Apple QuickTime/Darwin Streaming Server QTSSReflector Module Integer Overflow Vulnerability
BugTraq ID: 7659

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7659>

Summary:

The Darwin/QuickTime Streaming Servers are used as a web interface for Streaming Server configuration. They are available for the Linux, Solaris, Microsoft Windows and MacOS X operating systems.

A vulnerability has been reported for Apple Quicktime/Darwin Streaming Server. The problem is said to occur within the QTSSReflector module while processing the ANNOUNCE command. Specifically, by specifying the Content-Length of an ANNOUNCE request to 0xffffffff (4294967295) it may be possible to overflow an unsigned integer. As a result, an unexpected calculation may occur within the affected module, causing the server to crash. Due to the nature of the value that is supplied to Content-Length, this issue may actually be a result of signed/unsigned variable mismatching. This behavior however has not been confirmed.

It should be noted that it has been speculated that this issue may be exploitable to corrupt process memory. If so, it may be possible for an attacker to overwrite sensitive values in an attempt to execute arbitrary instructions with the privileges of the server.

Apple has confirmed that this issue may be exploitable to trigger a denial of service. However, it is believed that remote exploitability is unlikely as it would require an administrator to manually configure the service to permit unauthenticated broadcasts.

18. Apple QuickTime/Darwin Streaming MP3Broadcaster ID3 Tag Handling Vulnerability
BugTraq ID: 7660

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7660>

Summary:

The Apple QuickTime/Darwin MP3 Broadcaster is encoding software used to stream online broadcasts. They are available for the Linux, Solaris, Microsoft Windows and MacOS X operating systems.

MP3Broadcaster has been reported prone to a vulnerability when processing malformed ID3 tag information. The issue presents itself, under specific conditions, when the user invokes the MP3Broadcaster utility using the '-X -l' command line options, to generate a list based off malicious MP3 files. When a malformed integer within the ID3 data of a malicious MP3 file is processed, a miscalculation may occur which could potentially result in the corruption of process memory. This is likely due to

insufficient sanity checks performed when handling signed integer values contained within MP3 file ID3 tags.

Apple has confirmed that this issue may be exploitable to trigger a denial of service. However, it is believed that remote exploitability is unlikely, as it would require an administrator to manually configure the service to permit unauthenticated broadcasts.

19. Microsoft Internet Connection Firewall IPv6 Traffic Blocking Vulnerability

BugTraq ID: 7666

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7666>

Summary:

Microsoft provides firewall capabilities using its Internet Connection Firewall (ICF).

An issue has been reported for systems that have enabled ICF whereby certain traffic may bypass existing firewall filters. Specifically, it has been reported the ICF fails to block IPv6 traffic.

This may result in an administrator having a false sense of security.

20. Microsoft Netmeeting CALLTO URL Buffer Overflow Vulnerability

BugTraq ID: 7639

Remote: Yes

Date Published: May 20 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7639>

Summary:

Microsoft Netmeeting sessions can be launched through Internet Explorer by browsing to a 'callto:' link. These links usually contain the address of the Netmeeting user to be called and may also contain a directory to retrieve the addressing information from.

It has been reported that clicking on a malformed 'callto:' URI using Internet Explorer may result in Windows failing due to a kernel mode exception. This issue may be due to a boundary condition error in one of the parameters accepted by the CALLTO protocol handler.

Successful exploitation of this vulnerability may result in a denial of service to the system. If this is due to a boundary condition error, it is not currently known if critical memory is overwritten that could allow for code execution.

Symantec was unable to reproduce this vulnerability on a Windows 2000 SP3 system running Internet Explorer 6.0 SP1 and Netmeeting 3.01 using the supplied proof of concept code.

It is important to note that the CALLTO protocol handler does not function by default on browsers other than Internet Explorer.

** It has been reported that when Windows fails in this instance, a pointer may be overwritten. This indicates that code execution could be possible through successful exploitation of this vulnerability.

21. Microsoft Windows Media Player Automatic File Download and Execution Vulnerability

BugTraq ID: 7640

Remote: Yes

Date Published: May 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7640>

Summary:

Windows Media Player could allegedly allow files to be downloaded and executed without user intervention.

When a specifically crafted XMLNS (XML Name Space) URI is embedded within an HTML email message, a media file referenced in the URI may be automatically downloaded. If this is combined with the vulnerability described in BID 5543 (Microsoft Windows Media Player File Attachment Script Execution Vulnerability), a malicious script or executable file may be automatically downloaded and executed on the vulnerable system.

This vulnerability was reported to affect systems running Outlook Express 6.00.2800.1123 and Windows Media Player 7.01.00.3055 or 8.00.00.4487. Windows Media Player 9 series is said to be unaffected.

Symantec was unable to reproduce this vulnerability in testing with Outlook Express 6.00.2800.1123 and Windows Media Player 7.01.00.3055.

22. Demarc PureSecure Plaintext Password Vulnerability

BugTraq ID: 7650

Remote: No

Date Published: May 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7650>

Summary:

Demarc PureSecure is a commercially available graphical front-end for Snort, in addition to being a generalized network monitoring solution. Snort is a popular open-source NIDS (Network Intrusion Detection System). Demarc PureSecure will run on most Linux and Unix variants, as well as Microsoft Windows NT/2000/XP operating systems.

A problem with the Demarc PureSecure software could make unauthorized access to user credentials possible.

It has been reported that a problem exists in the method used in the storage of passwords by Demarc PureSecure. This could lead to users

gaining unauthorized access to passwords, and potentially unauthorized access to the central/remote logging server.

Specifically, Demarc PureSecure stores certain user passwords on the disk using plain-text format by default. A local user with access sufficient to read the files used by the Demarc PureSecure may disclose the usernames and passwords.

Information gathered in this way may be used to aid in further attacks launched against the vulnerable system.

It should be noted that although this vulnerability has been reported to affect Demarc PureSecure version 1.0.6 previous versions might also be affected.

23. Magic Winmail Server USER POP3 Command Format String Vulnerability

BugTraq ID: 7667

Remote: Yes

Date Published: May 23 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7667>

Summary:

Magic Winmail Server is a e-mail server designed for use on Microsoft Windows operating environments.

A format string vulnerability has been reported for Magic Winmail Server when processing the USER POP3 command.

An attacker may exploit this vulnerability by connecting to the vulnerable mail server and issuing the USER command with malicious format string specifiers. When the command is processed, the malicious format string specifiers may be interpreted. As a result, it may be possible for sensitive locations in memory to be corrupted. This may ultimately result in the execution of attacker-supplied code.

This vulnerability was reported for Magic Winmail Server 2.3.

IV. MICROSOFT FOCUS LIST SUMMARY

1. Windows 2003 Server – MS Rulez? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/322535>

2. Updated URLScan Security Tool Released (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/322305>

3. Netreg for Windows (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/322298>

4. Article Announcement: Passive Network Traffic Analysis: Understanding a Network Through Passive Monitoring (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/322175>

5. Administrivia: Sobig/Mankx/Palyh (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/321987>

6. SecurityFocus Microsoft Newsletter #137 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/321919>

7. Article Announcement: "Relax, It Was a HoneyPot" (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/321894>

8. Article Announcement: Malware Myths and Misinformation, Part One (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/321893>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. CryptoGram Secure Login

by CryptoGram SA

Platforms: Windows 2000, Windows NT, Windows XP

Relevant URL:

Summary:

As computer crime rises (computer theft, fraud, piracy, etc.) secure access to information has become a key factor in the architecture of computer systems. To combat these threats, only a hardware based authentication solution can fully protect access to your computers. With CryptoGram Secure Login, users must possess a token and provide information to be authenticated. Using the latest cryptographic and biometric technologies, the CryptoGram Secure Login solution protects access to your Windows NT 4.0, Windows 2000 and Windows XP computers and keeps all unauthorized users out

2. Tricryption Engine

by ERUCES

Platforms: N/A

Relevant URL:

Summary:

The ERUCES Tricryption Engine is an enabling technology platform based on the most advanced high-volume encryption and automated key management system on the market today. The Tricryption Engine is the only data security platform that can scale to meet the continually growing encryption requirements companies must implement. As organizations look for methods to protect increasing amounts of electronic data, they need to deploy solutions that will completely prohibit unauthorized users from reading or tampering with protected data, while at the same time remove the constraints of system performance and on-going management. With its patent-pending automated encryption key management process, the Tricryption Engine platform can be used to protect all types of electronic data, from databases to multimedia files.

3. neuSECURE

by GuardedNet

Platforms: Linux, UNIX, Windows 2000, Windows NT, Windows XP

Relevant URL:

Summary:

neuSECURE is a web-based security information management software solution designed to provide a comprehensive, coherent view of enterprise security. It correlates log data files from disparate machines such as firewalls, intrusion detection systems, computer systems and routers and automatically analyzes this data to uncover legitimate threats to the enterprise. neuSECURE allows security analysts to prioritize their investigations and focus on the mission-critical task of responding to threats as they are occurring, rather than after the damage is done. And with neuSECURE a security team can manage security threats from early detection to final resolution without ever leaving the intuitive, web-based console.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. WinCrypt v2.0

by C2SG

Relevant URL:

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

Platforms: Windows 2000, Windows 3.x, Windows 95/98, Windows NT, Windows XP

Summary:

This is desktop encryption software to stop prying eyes. Windows users can now secure documents in such a way that sensitive files on hard drives and

e-mail attachments are totally unreadable to unauthorized users.

Users can drag and drop sensitive files into the Wincrypt window, select a password, and then e-mail the file to the intended recipient. The only people able to read the document are the holders of the password. The file or folder is protected by 256-bit Advanced Encryption Standard (AES).

Advanced features include anti-logging keyboard, quik-klik encryption and self decrypting files.

2. Darik's Boot and Nuke v2003052000(Beta)

by Darik Horn

Relevant URL:

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

Platforms: Os Independent

Summary:

Darik's Boot and Nuke (DBAN) is a self-contained boot floppy that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction.

3. incident.pl v2.6

by Viraj Alankar

Relevant URL:

<http://www.cse.fau.edu/~valankar/>

Platforms: N/A

Summary:

incident.pl is a small script that, when given logs generated by snort, can generate an incident report for every event that appears to be an attempted security attack, and report the attack to the appropriate administrators.

VI. SPONSOR INFORMATION

This Issue is Sponsored By: SpiDynamics

ALERT: Top 10 Web Application Attack Techniques and Methods to Combat them
Learn why 70% of today's successful hacks involve Web Application attacks such as: SQL Injection, XSS, Cookie Manipulation, and Parameter Manipulation.

All undetectable by Firewalls and IDS!

Download *FREE* white paper from SPI Dynamics for a complete guide to protection!

Visit us at: <http://www.spidynamics.com/mktg/webappsecurity102>
