

SecurityFocus Microsoft Newsletter #176

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-02/0044.html>

From: Marc Fossi (mfossi_at_securityfocus.com)

Date: 02/17/04

Date: Tue, 17 Feb 2004 10:19:47 -0700 (MST)

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

SecurityFocus Microsoft Newsletter #176

This Issue is Sponsored by: Spidynamics

ALERT: Attacking SOAP Web Services and Methods of Protection White Paper. Are you vulnerable? This white paper will cover various types of attacks based on the SOAP implementation of Web services over HTTP and describes how you can shield your applications from these assaults. Learn how to defend against Web services attacks with real step-by-step examples of hacking methods such as: SQL Injection, Cross Site Scripting and Parameter Manipulation.

http://www.securityfocus.com/sponsor/SPIDynamics_ms-secnews_040216

I. FRONT AND CENTER

1. Wireless Honeypot Trickery
2. Automating Windows Patch Mngt: Part I

II. MICROSOFT VULNERABILITY SUMMARY

1. Multiple Oracle Database Parameter/Statement Buffer Overflow...
2. BolinTech Dream FTP Server User Name Format String Vulnerabi...
3. PHP-Nuke 'News' Module Cross-Site Scripting Vulnerability
4. Microsoft Internet Explorer LoadPicture File Enumeration Wea...
5. PHP-Nuke 'Reviews' Module Cross-Site Scripting Vulnerability
6. PHP-Nuke Public Message SQL Injection Vulnerability
7. Microsoft Windows XP HCP URI Handler Arbitrary Command Execu...
8. Microsoft Windows Internet Naming Service Buffer Overflow Vu...
9. Microsoft Internet Explorer Shell: IFrame Cross-Zone Scripti...
10. Microsoft Internet Explorer Double-Null URI Denial Of Servic...
11. PHPNuke Category Parameter SQL Injection Vulnerability
12. EvolutionX Multiple Remote Buffer Overflow Vulnerabilities
13. Microsoft Virtual PC For Mac Temporary File Privilege Escala...
14. Microsoft ASN.1 Library Length Integer Mishandling Memory Co...
15. Microsoft Baseline Security Analyzer Vulnerability Identific...
16. Microsoft Windows ASN.1 Library Bit String Processing Intege...
17. Samba Mksmbpasswd.sh Insecure User Account Creation Vulnerab...

18. Microsoft Internet Explorer Unauthorized Clipboard Contents ...
19. Ratbag Game Engine Denial of Service Vulnerability
20. Macallan Mail Solution Web Interface Authentication Bypass V...

III. MICROSOFT FOCUS LIST SUMMARY

1. PPTP versus L2TP and possible attacks (Thread)
2. PPTP versus L2TP and possible attacks – what next? (Thread)
3. Article Announcement: Wireless Honeypot Trickery (Thread)
4. Command Line Interface for Windows Server 2003 Zippe... (Thread)
5. Article Announcement: Automating Windows Patch Manag... (Thread)
6. MS04–006 patch.. error in verbage? (Thread)
7. Looking for SQL security details (Thread)
8. SecurityFocus Microsoft Newsletter #175 (Thread)
9. Looking for SQL security details (Version 2) (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Norton Internet Security 2004
2. Dekart Logon
3. AppSentry
4. AppDefend
5. Airscanner Mobile AntiVirus Pro
6. Symantec?s Norton Internet Security 2004 Professional

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Stunnel v4.05
2. Airscanner Mobile AntiVirus Pro v2.5
3. FileWatch v1.0
4. Enigmail v0.83.2
5. cosign v1.5
6. Jacksum v1.4.0

VI. UNSUBSCRIBE INSTRUCTIONS

VII. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Wireless Honeypot Trickery
By Laurent Oudot

This paper will introduce honeypots as a countermeasure for attacks on wireless environments using WiFi–related technologies. They can be used to identify and defeat unsuspecting blackhat attackers.

<http://www.securityfocus.com/infocus/1761>

2. Automating Windows Patch Mngt: Part I
By Jonathan Hassell

This article, the first in a three–part series, discusses Microsoft's Software Update Services (SUS) in depth, including installation, administration, and maintenance.

<http://www.securityfocus.com/infocus/1760>

II. MICROSOFT VULNERABILITY SUMMARY

1. Multiple Oracle Database Parameter/Statement Buffer Overflow...

BugTraq ID: 9587

Remote: Yes

Date Published: Feb 05 2004

Relevant URL: <http://www.securityfocus.com/bid/9587>

Summary:

Oracle is a commercial database product, which is available for a number of platforms including Microsoft Windows and Unix and Linux variants.

Oracle database has been reported prone to multiple buffer overflow vulnerabilities when processing certain parameters and functions. Specifically the TIME_ZONE parameter lacks sufficient boundary checks. Therefore an excessive value assigned to TIME_ZONE may potentially overrun the bounds of a buffer in stack-based memory. This may result in the corruption of memory adjacent to the affected buffer, and ultimately may provide for arbitrary code execution.

Additionally the NUMTOYMINTERVAL function has been reported prone to a buffer overflow vulnerability. The issue presents itself due to a lack of sufficient boundary checks performed on char_expr parameters passed as an argument to the function. Again this issue may be exploited by passing excessive data as the second argument to a NUMTOYMINTERVAL statement call.

The NUMTODSINTERVAL function has also been reported prone to a buffer overflow vulnerability. The issue again presents itself due to a lack of sufficient boundary checks performed on char_expr parameters passed as an argument to the function. This issue may be exploited in a similar manner to the NUMTOYMINTERVAL issue, by passing excessive data as the second argument to a NUMTODSINTERVAL statement call.

Finally the FROM_TZ function has been reported prone to a buffer overflow vulnerability. The issue will present itself when excessive data is passed as the third parameter of a properly formatted FROM_TZ statement call.

Any one of these issues may be exploited to execute arbitrary code with elevated privileges.

2. BolinTech Dream FTP Server User Name Format String Vulnerabi...

BugTraq ID: 9600

Remote: Yes

Date Published: Feb 07 2004

Relevant URL: <http://www.securityfocus.com/bid/9600>

Summary:

BolinTech Dream FTP Server is a multithreaded FTP server designed for Microsoft Windows platforms.

Dream FTP Server has been reported to be prone to a remote format string vulnerability when processing a malicious request from a client.

The vulnerability presents itself when the server receives a malicious request containing embedded format string specifiers from a remote client. Specifically, this issue occurs when supplying a username during FTP authentication. The source of the problem is incorrect use of a formatted printing function, which processes data supplied during FTP server authentication. As a result, format specifiers supplied in this manner will be interpreted literally and may result in attacker-specified memory being corrupted or disclosed.

Although it has been demonstrated that this could crash the server, the vulnerability could also theoretically allow for execution of arbitrary code on the system hosting the server. This would occur in the security context of the server process.

Dream FTP Server version 1.02 has been reported to be prone to this issue, however, it is possible that other versions may be affected by this issue as well.

3. PHP-Nuke 'News' Module Cross-Site Scripting Vulnerability

BugTraq ID: 9605

Remote: Yes

Date Published: Feb 09 2004

Relevant URL: <http://www.securityfocus.com/bid/9605>

Summary:

PHP-Nuke is a freeware content management system. Implemented in PHP, it is available for a range of systems, including Unix, Linux, and Microsoft Windows.

It has been reported that the PHP-Nuke 'News' module is prone to a cross-site scripting vulnerability. The issue arises due to the module failing to properly sanitize user-supplied information. The URI parameter 'title' 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 vulnerable web page. 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.

It has been reported that this issue affects versions 6.x – 7.x of the software, however earlier versions may also be vulnerable.

4. Microsoft Internet Explorer LoadPicture File Enumeration Wea...

BugTraq ID: 9611

Remote: Yes

Date Published: Feb 07 2004

Relevant URL: <http://www.securityfocus.com/bid/9611>

Summary:

Microsoft Internet Explorer is prone to an issue that may permit a remote site to enumerate the existence of files on the client system.

This may be exploited via abuse of the VBScript LoadPicture method. This function is typically used to load an image by returning a reference to a picture object. The return value of this method will disclose enough information to determine whether a file requested via the method exists on the system or not. The source of this issue appears to be that the method does not adequately verify whether the requested resource is of a graphical format supported by the method (such as .bmp, .ico, .jpg, etc.). As a result, the method may be called on any resource and will return information as to whether the resource was successfully loaded or not.

A malicious web page could call the vulnerable method to gather information about whether or not particular files exist on the victim's system. Exploitation of the weakness may assist in other attacks which depend on the attacker being able to determine whether or not certain files on the system exist.

5. PHP-Nuke 'Reviews' Module Cross-Site Scripting Vulnerability

BugTraq ID: 9613

Remote: Yes

Date Published: Feb 09 2004

Relevant URL: <http://www.securityfocus.com/bid/9613>

Summary:

PHP-Nuke is a freeware content management system. Implemented in PHP, it is available for a range of systems, including Unix, Linux, and Microsoft Windows.

It has been reported that the PHP-Nuke 'Reviews' module is prone to a cross-site scripting vulnerability. The issue arises due to the module failing to properly sanitize user-supplied information. The URI parameter 'title' 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 vulnerable web page. 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.

It has been reported that this issue affects versions 6.x – 7.x of the software, however earlier versions may also be vulnerable.

6. PHP-Nuke Public Message SQL Injection Vulnerability

BugTraq ID: 9615

Remote: Yes

Date Published: Feb 09 2004

Relevant URL: <http://www.securityfocus.com/bid/9615>

Summary:

PHP-Nuke is a freeware content management system. Implemented in PHP, it is available for a range of systems, including Unix, Linux, and Microsoft Windows.

It has been reported that the 'public message' feature of PHP-Nuke is vulnerable to an SQL injection vulnerability. The issue is due to a failure to properly sanitize the '\$p_msg' parameter in the 'public_message()' function of the '/mainfile.php' script.

As PHP-Nuke forces all variables to be global within the context of the application, the '\$p_msg' parameter may be specified in either POST, GET or COOKIE data. Within the 'public_message()' function, the '\$p_msg' parameter is decoded into the '\$c_mid' parameter, which is directly used in the generation of the SQL query. An attacker could use an SQL Union command passed via the '\$p_msg' parameter to mine data from the database.

As a result of this issue an attacker could modify the logic and structure of database queries. Other attacks may also be possible, such as gaining access to sensitive information.

It has been reported that this issue affects versions 6.x – 7.x of the software, however earlier versions may also be vulnerable.

7. Microsoft Windows XP HCP URI Handler Arbitrary Command Execu...

BugTraq ID: 9621

Remote: Yes

Date Published: Feb 09 2004

Relevant URL: <http://www.securityfocus.com/bid/9621>

Summary:

A local Help and Support Center application was introduced with Microsoft Windows XP. It is an extended version of Help Center applications included in previous versions of the operating system. An associated protocol handler 'hcp:/' is supported in Windows XP and may be invoked via Internet Explorer.

The Microsoft Windows XP HCP URI handler has been reported prone to a vulnerability that may provide for arbitrary command execution. The issue is alleged to present itself when a specially formatted HCP URI that references a local resource is processed. If an attacker crafts a malicious HCP URI that references local content using a file:/// URI, it may be presented to an unsuspecting user, when this link is followed arbitrary commands may be invoked in the context of the user who followed the link.

This issue could also permit remote sites to be opened in the context of the Local Zone, though this has not been confirmed.

This issue has been reported to be present in Polish versions of Windows XP SP1; other versions may also be vulnerable. Symantec has not been able to reproduce this behavior.

8. Microsoft Windows Internet Naming Service Buffer Overflow Vu...

BugTraq ID: 9624

Remote: Yes

Date Published: Feb 10 2004

Relevant URL: <http://www.securityfocus.com/bid/9624>

Summary:

The Microsoft Windows Internet Name Service (WINS) allows the mapping of NetBIOS names to IP addresses and vice-versa. WINS servers can allow users to browse for local resources on the network using computer names.

The WINS service is prone to a stack-based buffer overflow.

This issue exists because WINS fails to correctly validate the length of specially crafted packets received by the service. Exploitation of this vulnerability has different effects depending upon the Windows version running the service.

On Windows NT 4.0 and 2000, the WINS service will perform additional processing, but will return to a normal state after a short period. The service does not fail on these platforms when receiving malformed packets, however, a constant stream of these packets could reduce system performance.

On Windows 2003, these malformed packets will cause the WINS service to fail. The service will automatically restart, but if the service fails again after a third restart, it must be restarted manually. The denial of service occurs on Windows 2003 due to a security feature used during development called the /GS flag. This feature is meant to detect stack-based buffer overflow exploitation attempts and reduce the possibilities of successful exploitation. In this case, the /GS flag terminates the service in order to prevent arbitrary code execution. It has been conjectured that if an attacker were to find a way to bypass this security feature, exploitation could result in the execution of arbitrary code on the vulnerable system. Code execution would likely occur in the security context of WINS.

9. Microsoft Internet Explorer Shell: IFrame Cross-Zone Scripti...

BugTraq ID: 9628

Remote: Yes

Date Published: Feb 10 2004

Relevant URL: <http://www.securityfocus.com/bid/9628>

Summary:

It has been alleged that Microsoft Internet Explorer is prone to an issue that may allow hostile script code to access properties of an IFrame that has been opened in the context of the My Computer Zone. Reportedly, if an IFrame opens up a local resource using a 'shell:' link, it may be possible for the page that spawns the IFrame to access properties of the My Computer Zone. If this issue is exploitable, this could ultimately lead to execution of malicious script code in the context of the My Computer Zone, potentially allowing for remote compromise of the client system in the context of the client user.

These reports have not been confirmed by Symantec and are pending further investigation. This BID will be updated when further information becomes available and retired if the alleged issue is not exploitable.

10. Microsoft Internet Explorer Double-Null URI Denial Of Servic...

BugTraq ID: 9629

Remote: Yes

Date Published: Feb 10 2004

Relevant URL: <http://www.securityfocus.com/bid/9629>

Summary:

A problem in the handling of URIs with double nulls has been reported in Microsoft Internet Explorer. Because of this, it may be possible for a remote attacker to deny service to legitimate users of an affected system.

The problem is in the handling of URIs with double null characters (encoded as %00) at the end of a URI. Reports indicate that it is possible for remote websites to take advantage of this issue by forcing a user to load a maliciously-crafted URI. Upon exploitation of this issue by a remote site, the host system executing the browser becomes resource-bound, experiencing a 100% consumption of processor resources, and ultimately freezing up entirely.

This issue has been reported to occur with only specific host names, and only on systems that do not first pass requests through a web proxy server. A pattern of host names that identifies the scope of this issue is currently not available. This issue has also been reported to not occur when the "Do not save encrypted pages to disk" option is enabled, which is not the default configuration.

Additionally, this option is conjectured to be an issue in a library component within the browser, as this issue affects Microsoft Internet Explorer and Microsoft Outlook. This would also likely affect any other system components that invoke the browser.

11. PHPNuke Category Parameter SQL Injection Vulnerability

BugTraq ID: 9630

Remote: Yes

Date Published: Feb 10 2004

Relevant URL: <http://www.securityfocus.com/bid/9630>

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.

A vulnerability has been reported to exist in PHPNuke that may allow a remote attacker to inject malicious SQL syntax into database queries. The source of this issue is insufficient sanitization of user-supplied input.

The problem is reported to exist in the \$category variable contained within the 'index.php' page. It has been reported that \$category is not sanitized for user-supplied input before it is included in SQL queries that are later executed by the database. A remote attacker may exploit this issue while performing a search in 'index.php' to influence SQL query logic.

A malicious user may influence database queries in order to view or modify sensitive information, potentially compromising the software or the database. It has been reported that an attacker may be able to disclose the administrator password hash by exploiting this issue.

PHPNuke versions 6.9 and prior have been reported to be prone to this issue, however other versions may be affected as well.

12. EvolutionX Multiple Remote Buffer Overflow Vulnerabilities

BugTraq ID: 9631

Remote: Yes

Date Published: Feb 10 2004

Relevant URL: <http://www.securityfocus.com/bid/9631>

Summary:

EvolutionX is illegal software that is used to replace default Microsoft XBOX software.

The FTP server that is distributed with EvolutionX has been reported prone to multiple buffer overflow vulnerabilities. The first of these vulnerabilities exists post-authentication, and is due to a lack of sufficient bounds checking performed on arguments that are passed to the 'cd' command. It has been conjectured that an attacker who is authenticated to the FTP server may potentially exploit this condition to execute arbitrary code in the context of the affected service. Immediate consequences of a failed exploit attempt may result in the XBOX appliance behaving in an unstable manner, or potentially becoming unresponsive until the appliance is power-cycled.

The second issue exists pre-authentication, excessive data passed as username:password combination to the affected FTP server will trigger the buffer overrun. Again, due to the nature of this issue, it has been conjectured that an attacker may potentially exploit this condition to execute arbitrary code in the context of the affected service. Again immediate consequences of a failed exploit attempt may result in the XBOX appliance behaving in an unstable manner, or potentially becoming unresponsive until the appliance is power-cycled.

Finally the telnet server that is distributed with EvolutionX has been reported prone to a buffer overflow vulnerability when handling excessive data passed as an argument to the 'dir' command. An attacker may exploit this buffer overflow to deny service to legitimate users of the XBOX appliance, again it has been conjectured that this issue may be exploitable to result in arbitrary code execution.

It should be noted that while this vulnerability has been reported to affect EvolutionX builds 3921 and 3935, other versions might also be affected.

13. Microsoft Virtual PC For Mac Temporary File Privilege Escala...

BugTraq ID: 9632

Remote: No

Date Published: Feb 10 2004

Relevant URL: <http://www.securityfocus.com/bid/9632>

Summary:

Microsoft Virtual PC For Mac is an x86 emulator for Apple Mac OS systems.

Microsoft has reported an issue in Virtual PC for Mac that may permit a local attacker to gain elevated privileges on a system hosting the software.

This is due to insecure handling of temporary files by the setuid root VirtualPC_Services binary, potentially permitting a malicious local user to create a malicious symbolic link in place of the temporary file (/tmp/VPCServices_Log). This symbolic link could be constructed to point to a sensitive system file. When the software is executed, operations intended to be performed on the temporary file will instead be performed on the file pointed to by the symbolic link, causing such a file to be corrupted. Alternatively, if the symbolic link points to a non-existent file, this file would be created with the attacker's umask settings. Exploitation could result in corruption of sensitive files and elevation to root privileges.

14. Microsoft ASN.1 Library Length Integer Mishandling Memory Co...
BugTraq ID: 9633

Remote: Yes

Date Published: Feb 10 2004

Relevant URL: <http://www.securityfocus.com/bid/9633>

Summary:

Microsoft Windows Abstract Syntax Notation 1 (ASN.1) handling Library (MSASN1.dll) is shipped as a part of the Microsoft Windows Operating System. The MSASN1 library provides an application programmer's interface into Microsoft ASN.1 encoding/decoding and processing functions.

A vulnerability has been reported in the Microsoft ASN.1 library. This issue is related to insufficient checking of data supplied via an externally supplied length field in ASN.1 BER encoded data.

In particular, ASN.1 BER encoded data consists of a tag number that specifies how following value data is interpreted, followed by a length field for that data and then the actual data itself. Supplying an excessive length field value in the range of 0xFFFFFFFFD to 0xFFFFFFFF will result in an integer overflow during a heap allocation operation. Despite checks on the length field, there is a separate pointer arithmetic overflow that occurs in the length verification routine itself that could cause large amounts of heap memory to be corrupted. This occurs because the internal ASN1BERDecCheck() length verification function will be bypassed when length field values in the range of 0xFFFFFFFFD to 0xFFFFFFFF are supplied and then subsequent memory allocation and copying operations will be performed with excessive values. This could be leveraged to corrupt sensitive values in memory, resulting in execution of arbitrary code.

The following specific decoder functions are known to be vulnerable to this issue:

ASN1BerDecCharString
ASN1BERDecChar16String
ASN1BERDecChar32String
ASN1BERDecEoid
ASN1BERDecGeneralizedTime
ASN1BERDecMultibyteString
ASN1BERDecOctetString
ASN1BERDecOpenType
ASN1BERDecSXVal
ASN1BERDecUTCTime
ASN1BERDecUTF8String
ASN1BERDecZeroCharString
ASN1BERDecZeroChar16String
ASN1BERDecZeroChar32String
ASN1BERDecZeroMultibyteString

This vulnerability is exposed in a number of security related operating system components, including Kerberos (via UDP port 88), Microsoft IIS with SSL support enabled and NTLMv2 authentication (via TCP ports 135, 139 and 445). Other components may also be affected, though a comprehensive list is not available at this time. Client applications which use the library will be affected, including LSASS.EXE and CRYPT32.DLL (and any application that relies on CRYPT32.DLL). The vulnerable library is used frequently in components that handle certificates such as Internet Explorer and Outlook. Handling of signed ActiveX components could also present an exposure.

It should be noted that because ASN.1 data will likely be encoded, for example Kerberos, SSL, IPSec or Base64 encoded, the malicious integer values may be obfuscated and as a result not easily detectable.

This vulnerability was originally covered in BID 9626, but further information has been made available which identifies a number of distinct vulnerabilities in the library and so this specific issue has been assigned an individual BID.

15. Microsoft Baseline Security Analyzer Vulnerability Identific...

BugTraq ID: 9634

Remote: No

Date Published: Feb 10 2004

Relevant URL: <http://www.securityfocus.com/bid/9634>

Summary:

Microsoft Baseline Security Analyzer (MBSA) is a tool which scans a Microsoft Windows system and creates a security report including a variety of information about the target system.

A weakness has been identified in MBSA. It has been reported that under some circumstances MBSA may not properly identify security vulnerabilities in the target operating system. Various tests have revealed this

condition occurs when a patch has been installed on a machine but the machine has not been rebooted therefore leaving the host operating system vulnerable. The weakness in MBSA causes the scanner to still identify the host operating system as invulnerable. This issue may cause a false sense of security resulting in leaving the operating system prone to security vulnerabilities.

Microsoft Baseline Security Analyzer version 1.2 is assumed to be affected by this issue, however, it is possible that other versions are affected by this flaw as well.

16. Microsoft Windows ASN.1 Library Bit String Processing Intege...

BugTraq ID: 9635

Remote: Yes

Date Published: Feb 10 2004

Relevant URL: <http://www.securityfocus.com/bid/9635>

Summary:

Microsoft Windows Abstract Syntax Notation 1 (ASN.1) handling Library (MSASN1.dll) is shipped as a part of the Microsoft Windows Operating System. The MSASN1 library provides an application programmer's interface into Microsoft ASN.1 encoding/decoding and processing functions.

Microsoft ASN.1 handling library has been reported prone to an integer overflow vulnerability that may result in arbitrary heap-based memory corruption. The issue presents itself in the ASN.1 BER decoding/encoding routines, specifically the ASN1BERDecBitString() function.

ASN1BERDecBitString() handles constructed bit strings by concatenating each of the simple bit strings that comprise the compound one. The integer overflow occurs when a bit string is processed and the number of bits in the bit string is added to the cumulative total as follows:

```
lea eax, [ecx+eax+7]
```

This may provide a conduit for an attacker to trigger a boundary condition error. When the first bit string processed by ASN1BERDecBitString possesses a specified signed length of 0xfffff9(-7), and then the aforementioned arithmetic (ecx+eax+7) sums the accumulated bits (0) with the signed length of the bit string (-7). The rounding value (+7) is then added to the total. This will result in a total assigned length of zero.

It has been reported that this value is then further processed by the DecMemReAlloc() function call, and ultimately results in a zero-byte chunk being allocated on the heap. The original bit string lengths are passed to the function ASN1bitcpy(). This function later performs a memcpy() operation to copy supplied bit string data into the zero-byte allocated heap based buffer. This operation will result in the corruption of heap based management structures, and may ultimately be leveraged by an attacker to have arbitrary code executed in the context of the affected process.

This vulnerability is exposed in a number of security related operating system components, including Kerberos (via UDP port 88), Microsoft IIS

with SSL support enabled and NTLMv2 authentication (via TCP ports 135, 139 and 445). Other components may also be affected, though a comprehensive list is not available at this time. Client applications which use the library will be affected, including LSASS.EXE and CRYPT32.DLL (and any application that relies on CRYPT32.DLL). The vulnerable library is used frequently in components that handle certificates such as Internet Explorer and Outlook. Handling of signed ActiveX components could also present an exposure.

It should be noted that because ASN.1 data will likely be encoded, for example Kerberos, SSL, IPSec or Base64 encoded, the malicious integer values may be obfuscated and as a result not easily detectable.

This vulnerability was originally covered in BID 9626, but further information has been made available which identifies a number of distinct vulnerabilities in the library and so this specific issue has been assigned an individual BID.

17. Samba Mksmbpasswd.sh Insecure User Account Creation Vulnerab...

BugTraq ID: 9637

Remote: Yes

Date Published: Feb 10 2004

Relevant URL: <http://www.securityfocus.com/bid/9637>

Summary:

Samba is a freely available file and printer sharing application maintained and developed by the Samba Development Team. Samba allows file and printer sharing between operating systems on the Unix and Microsoft platforms. Samba ships with several helper scripts, one of these scripts is mksmbpasswd.sh, which is used to aid in user account creation.

The mksmbpasswd.sh shell script is reported prone to a vulnerability. The issue results in the creation of insecure user accounts. Specifically it has been reported that a password initialization problem in the mksmbpasswd.sh shell script results in user accounts being created with insecure passwords.

The issue surrounds the passwords for disabled user accounts. In some cases the affected script may overwrite these passwords with uninitialized memory. If an attacker were able to ascertain the contents of memory used to overwrite disabled account passwords they may be able to gain unauthorized access.

A remote attacker may exploit this issue by accessing a Samba share using an insecure account that was created using the affected script.

18. Microsoft Internet Explorer Unauthorized Clipboard Contents ...

BugTraq ID: 9643

Remote: Yes

Date Published: Feb 11 2004

Relevant URL: <http://www.securityfocus.com/bid/9643>

Summary:

A vulnerability was reported in Microsoft Internet Explorer that could permit a remote site to gain access to contents of the client user's clipboard.

This vulnerability is a variant of similar issues which could permit scripting operations to gain access to clipboard contents, such as that described in BID 215 and 3862. This issue employs the `execCommand("Paste")` method to copy clipboard contents into small (or hidden) textarea. Some of this functionality is legitimate and can be mitigated by disabling the "Allow paste options via scripting" scripting setting in the browser. However, it does appear that Internet Explorer does make some attempt to prevent this operation even when the option is enabled and so this issue does present a security risk because it demonstrates a means of bypassing these checks. In particular, the paste operation will fail if it attempts to paste clipboard contents into a `TextRange` that is non-displayed using either a CSS display property of "none" or an HTML input-type property of "hidden". Conversely, the operation does succeed if clipboard contents are pasted into a textarea that is either 1x1 pixel in size or with a visibility property of "hidden".

The impact of exploitation depends entirely on what sort of information is stored in the user's clipboard at the time of exploitation, though it is common for user's to copy various credentials into their clipboard. It should be noted that there will not be any context for the disclosed clipboard contents so the attacker will have to make assumptions as to whether the information is of a sensitive nature or not.

19. Ratbag Game Engine Denial of Service Vulnerability

BugTraq ID: 9644

Remote: Yes

Date Published: Feb 11 2004

Relevant URL: <http://www.securityfocus.com/bid/9644>

Summary:

Ratbag develops PC games for Microsoft Windows platforms. Ratbag games include Dirt Track Racing, Dirt Track Racing Australia, Leadfoot, Dirt Track Racing Sprint Cars, Dirt Track Racing 2, and World of Outlaws Sprint Cars.

A denial of service vulnerability has been identified in the software that may allow a remote attacker to cause a vulnerable server to crash or hang. The issue is reported to present itself due to excessive CPU usage caused by improper validation of user supplied data.

It has been reported that the server calculates the amount of data to be received from a user by analyzing a 16 bit value located at the beginning of each data block. This value is also used to calculate the amount of received data during transfer. An attacker may cause the server to enter an infinite loop by manipulating this value to a number of bytes that is greater than the actual data to be transferred to the server.

20. Macallan Mail Solution Web Interface Authentication Bypass V...

BugTraq ID: 9646

Remote: Yes

Date Published: Feb 12 2004

Relevant URL: <http://www.securityfocus.com/bid/9646>

Summary:

Macallan Mail Solution is a mail server for Microsoft Windows operating systems.

A vulnerability has been reported in Macallan Mail Solution that may permit remote attackers to bypass authentication for the web interface. This may be exploited by submitting a specially crafted HTTP GET request for the administration page of the web interface. Reportedly, if the request contains an extra slash when specifying the administration page (for example: //admin.html) then authentication will be bypassed.

There are conflicting reports from the vendor that state that the attacker will not be able to perform any administrative actions after bypassing authentication. This could threaten other security properties, such as exposing sensitive information, though this has not been confirmed.

III. MICROSOFT FOCUS LIST SUMMARY

1. PPTP versus L2TP and possible attacks (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/353984>

2. PPTP versus L2TP and possible attacks – what next? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/353982>

3. Article Announcement: Wireless Honeypot Trickery (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/353981>

4. Command Line Interface for Windows Server 2003 Zippe... (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/353790>

5. Article Announcement: Automating Windows Patch Manag... (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/353605>

6. MS04-006 patch.. error in verbage? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/353351>

7. Looking for SQL security details (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/353283>

8. SecurityFocus Microsoft Newsletter #175 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/353282>

9. Looking for SQL security details (Version 2) (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/353277>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Norton Internet Security 2004

By: Symantec

Platforms: Windows 95/98

Relevant URL: http://www.symantec.com/sabu/nis/nis_pe/

Summary:

Symantec's Norton Internet Security 2004 provides essential protection from viruses, hackers, and privacy threats. Powerful yet easy to use, this award-winning suite now includes advanced spam-fighting software to filter unwanted mail out of your inbox. Protect yourself, your family, and your PC online with Norton Internet Security 2004.

2. Dekart Logon

By:

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

Relevant URL: http://www.dekart.com/products/authentication_access/logon/

Summary:

Dekart Logon is a solution designed to provide an additional level of security for the Microsoft Windows operating system. Access to the Windows environment can only be gained after inserting a USB key or smart card into the appropriate slot and by entering the correct PIN code.

Dekart Logon offers a number of security options: you can select to have Windows access blocked once the key is removed, during a screen saver timeout or other user assigned prompts. This flexibility automatically reduces the possibility of human error by maintaining predefined security levels even if the user leaves their PC unattended.

3. AppSentry

By: Integrigy

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

Relevant URL: <http://www.integrigy.com/appsentry.htm>

Summary:

AppSentry is a new generation of security scanner and vulnerability assessment tool. Unlike other security scanners, AppSentry knows the application it is validating ? its technology and data model. The security audits and checks are written specifically for the application being tested. Hackers and mischievous employees often exploit security issues at different layers of the technology stack, thus only a complete and comprehensive security validation will uncover all risks in a multi-tiered environment.

The advantage of AppSentry is now you don't have to separate tools for the operating system, web server, and database. AppSentry is a single tool that can validate and audit the security of the entire application technology stack from operating system to application layer.

AppSentry is available for the following applications –

Oracle E-Business Suite (11i)

Oracle Database (8.x, 8i, 9i, 10g)

Oracle Application Server (9iAS, 10g)

SAP

PeopleSoft

Microsoft SQL Server

4. AppDefend

By: Integrigy

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

Relevant URL: <http://www.integrigy.com/appdefend.htm>

Summary:

AppDefend is a new concept in Intrusion Prevention – direct application protection. AppDefend protects the application from attacks and intrusions by blocking attacks before they reach the application.

AppDefend is designed specifically for the application it is protecting. Thus, when implementing for the Oracle E-Business Suite, there is no analysis or other configuration required to provide maximum protection for the application. Integrigy has already performed all this work for you — all modules, all versions.

AppDefend is designed to be simple to install and easy to maintain. A straight-forward, yet robust, implementation takes only 15 minutes. No complex configuration or analysis of the application is required.

5. Airscanner Mobile AntiVirus Pro

By: Airscanner Corp.

Platforms: Windows CE

Relevant URL: <http://airscanner.com/downloads/av/av.html>

Summary:

Airscanner Mobile AntiVirus Pro will quarantine or eradicate embedded viruses and malware, has fast, optimized scanning speed based on patent pending technology, has automatic, online updates of virus signatures and scanning engine as well as support for PocketPC 2003/Windows Mobile 2003 and easy online updates.

In addition to an accurate virus scanner, Airscanner Mobile AntiVirus includes these powerful tools for debugging Trojan horses:

- Intercept memory resident viruses with an advanced process discovery tool.
- Debug Trojan hacks with an easy-to-use registry viewer.
- Uncover denial of service attacks with a rapid system analyzer.
- Enter your own custom virus signatures (for experts).
- Perform fast, recursive, and flexibly multithreaded filesystem scanning.

6. Symantec's Norton Internet Security 2004 Professional

By: Symantec

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

Relevant URL: http://www.symantec.com/smallbiz/nis_pr/

Summary:

Symantec's Norton Internet Security 2004 Professional protects you and your business from online threats. It eliminates viruses automatically, blocks hackers, safeguards your personal information, fights spam, increases online productivity, recovers lost or damaged files, and thoroughly deletes confidential data you no longer need. Available in 5 and 10-user Small Office Packs.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Stunnel v4.05

By: Michal Trojnara, <Michal.Trojara@mirt.net>

Relevant URL: <http://stunnel.mirt.net/>

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

Summary:

The stunnel program is designed to work as an SSL encryption wrapper between remote client and local (inetd-startable) or remote server. It can be used to add SSL functionality to commonly used inetd daemons like POP2, POP3, and IMAP servers without any changes in the programs' code. It will negotiate an SSL connection using the OpenSSL or SSLeay libraries. It calls the underlying crypto libraries, so stunnel supports whatever cryptographic algorithms you compiled into your crypto package.

2. Airscanner Mobile AntiVirus Pro v2.5

By: Airscanner Corp

Relevant URL: <http://airscanner.com/downloads/av/av.html>

Platforms: Windows CE

Summary:

Airscanner Corporation is the most trusted name in helping to defend your mobile device from "airborne" computer viruses. From the company that wrote the best-selling technical book Maximum Wireless Security comes a professional strength virus scanner for the Pocket PC.

With the increased wireless connectivity of PDAs and Smartphones comes an increased threat from virus attacks. Save money, time, and data by protecting your valuable Pocket PC now with Airscanner Mobile AntiVirus Pro.

3. FileWatch v1.0

By: robinkeir@foundstone.com

Relevant URL: www.foundstone.com/rdlabs/tools.html

Platforms: Windows NT

Summary:

A file change monitor. Used with BlackICE Defender. FileWatch (originally called ICEWatch 1.x) is a small utility that can monitor a given file for changes. Monitoring can detect file size changes or simply file writes, both with minimal impact on system resources (no polling is performed). The primary use of this utility is for monitoring changes in the log file of a personal firewall program and being able to spawn a separate application when changes are detected, but the tool can be applied to any number of other uses.

4. Enigmail v0.83.2

By: Patrick

Relevant URL: <http://enigmail.mozdev.org/thunderbird.html>

Platforms: Linux, MacOS, POSIX, UNIX, Windows 2000, Windows 3.x, Windows 95/98, Windows CE, Windows NT, Windows XP

Summary:

Enigmail is a "plugin" for the mail client of Mozilla and Netscape 7.x which allows users to access the authentication and encryption features provided by the popular GnuPG software. Enigmail can encrypt/sign mail when sending, and can decrypt/authenticate received mail. It can also import/export public keys. Enigmail supports both the inline PGP format and the PGP/MIME format, which can be used to encrypt attachments. Enigmail is cross-platform, although binaries are supplied only for a limited number of platforms. Enigmail uses inter-process communication to execute GPG to carry out encryption/authentication.

5. cosign v1.5

By: UMich Web Team

Relevant URL: <http://weblogin.org/>

Platforms: UNIX, Windows 2000, Windows NT

Summary:

cosign is a Web single sign on system that allows users to authenticate once per session and access any protected Web resources at the institution. If used, passwords are sent only to a single, central URL.

Sessions have both idle and hard timeouts, and users can logout of all protected services by visiting a single URL. The use of public key cryptography ensures that a compromise of a protected Web server has no impact on the security of other participating servers.

6. Jacksum v1.4.0

By: jonelo

Relevant URL: <http://www.jonelo.de/java/jacksum/index.html>

Platforms: Linux, MacOS, Os Independent, OS/2, POSIX, Solaris, SunOS, UNIX, Windows 2000, Windows 95/98, Windows NT

Summary:

Jacksum is a free checksum utility entirely written in Java. It supports most common checksum algorithms (Adler32, BSD sum, POSIX cksum, CRC-16, CRC-32, MD2, MD5, SHA, and Unix System V sum).

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

This Issue is Sponsored by: Spidynamics

ALERT: Attacking SOAP Web Services and Methods of Protection- White Paper
Are you vulnerable? This white paper will cover various types of attacks based on the SOAP implementation of Web services over HTTP and describes how you can shield your applications from these assaults Learn how to defend against Web services attacks with real step- by- step examples of hacking methods such as: SQL Injection, Cross Site Scripting and Parameter Manipulation.

http://www.securityfocus.com/sponsor/SPIDynamics_ms-secnews_040216

Free trial: Astaro Security Linux --- firewall with Spam/Virus Protection

Protect your network with the comprehensive security solution that integrates six applications for ease of use and lower TCO.

Firewall - Virus protection - Spam protection - URL blocking - VPN
- Wireless security.

Download 30-day evaluation at:

<http://www.astaro.com/php/contact/securityfocus.php>
