Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Breakdown of the Top Five Windows 2000 IIS Threats in 2001

The author presents a detailed examination of the top five Windows IIS threats (2001): Remote Command Execution Via Internet Printing Service, Microsoft IIS CGI Filename Decode Error Vulnerability, Remote command execution via Buffer Overflow in Indexing Service, Unauthorised SMTP relaying, Buffer Overflow in FrontPage server extension.

Copyright SANS Institute

Author Retains Full Rights

AD

A Breakdown of the Top Five Windows 2000 IIS Threats in 2001

Simon P. Plant, CISSP
August 18th, 2001

Index

1. Remote Command Execution Via Internet Printing Service
2. Microsoft IIS CGI Filename Decode Error Vulnerability
3. Remote command execution via Buffer Overflow in Indexing Service
4. Unauthorised SMTP relaying
5. Buffer Overflow in FrontPage server extension

As a precursor to the following top five threats identified, the following best practices for running Internet Information Services 5.0 are:

- Apply the high security template policy called "hisecweb.inf"
- Observe the best practices for hardening IIS [1] from Microsoft
- Apply all the recommendations in "Secure Internet Information Services 5.0 Checklist" [2] during the install and configure stage of set-up
- Use the new Microsoft Hotfix (`hfnetchk.exe`) [3] tool to monitor patch updates from Microsoft. Schedule it to run daily
- Install Host IDS on all servers, especially in the DMZ
- Install a local firewall on every host
- Install anti-virus server scanners on all hosts
- Deploy firewalls and VPN's on the network perimeter
- Place IDS Nodes within the internal or private segment of the network
- Authenticate administrators and users with elevated privileges with dual authentication

The following five vulnerabilities discussed here are key to securing the most publicised exploit channels against Windows 2000 IIS servers in 2001. Through addressing these issues through a structured approach to intelligence gathering, it is possible to patch the servers in a knowledgeable way and ensure system stability.

1. Remote Command Execution Via Internet Printing Service

CERT advisory	CA-2001-10
CVE	CAN-2001-0241
Microsoft Bulletin	MS01-023
Initially discovered by:	EEye Digital Security (Riley Hassell)

Internet Printing is a new feature in Windows, introduced with the release of Windows 2000 Server. It provides users with the ability to access a printer across an Intranet or the Internet and submit a job directly to the printer through the browser. Printers are accessed using a URL in the address bar of the browser, such as

Internet Printing uses IPP (Internet Printing Protocol, an IETF standard [5]) as its low-level protocol, which is encapsulated within HTTP as the carrier. In Windows 2000, Microsoft have implemented Internet printing as an ISAPI server extension called ".printer". ISAPI filters are an Internet API for extending Internet Information Server using DLL's that allow pre-processing of requests and post-processing of responses. It is important to note that this service is implemented *by default* as part of the standard IIS installation.

The vulnerability exists in an unchecked buffer in the `msw3prt.dll`, allowing an attacker to post a string of approximately 420 characters that will cause the buffer to overflow and commands to be overwritten with the newly injected shell code. The vulnerability is

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

particularly severe because the IIS server will be running as the *system* user with highly elevated privileges.

Is It Running?
Is the Windows 2000 running Internet Information Server? If you have chosen the default install and not made any modifications, chances are the IPP service is running. Connect to the host using a web browser (pref. IE4+) and request:

```
http://host.example.com/printers, or
http://host.example.com/HPLaserJ       ## If HP printer shared
```

Access the port directly:

```
Telnet (or nc) host.example.com 80
GET /NULL.printer HTTP/1.1
Host: localhost            (CRLF x 2)
```

If the host is vulnerable, the server will return `HTTP/1.1 500` showing the service is active. If the ISAPI mappings have been removed, IIS will return `HTTP/1.1 404`, or a null response will mean the vulnerability has been patched.

Is It Required?
Firstly, check if the service is being used currently. Review the IIS log files (`%system32\Logfiles\w3svc1\ex`*`yymmdd`*`.log and archived logs`) either manually reading the logs, by opening the log file in notepad and CTL_F searching for the above entries, or using a log analyser such as Webtrends and looking for entries on "/printers" and "GET /Null.printer".

Next, check that the host has a shared printer connected to it. If so, IPP services may well be required. Most web servers however do not have printers attached, and the service can be easily disabled.

Are any applications using the service? Again, log files should show you, but check with the owner of the host and the development team responsible applications on the box.

The last check is :

```
> Load MMC.exe
> Add/Remove Snap-in and click Add in bottom left corner
> Select IIS Snap-in, Add & Close
> Under Internet Information Services, right-click the host
> Select Properties, and click Edit, WWW Service
> Go to the Home Directory tab, and click configuration near the
bottom right
> Scroll down and check for ".printer, %system32% \msw3prt.dll and GET
POST methods"
```

If the IPP service is enabled, the mapping will be available.

Addressing the Vulnerability
All Windows 2000 server versions Service Pack 2 and less are vulnerable if using the default installation, as well as Windows 2000 Professional workstations and Windows XP Beta IIS 6.0. Addressing the Printing Service vulnerability requires a number of steps.

1. Apply the Microsoft patch from `http://www.microsoft.com/Windows2000/downloads/critical/q296576/download.asp`. The patch file is called `Q296576_W2K_SP2_x86_en.EXE` under Windows 2000.

   Verify that the patches have been installed on the host:
   To verify that the patch has been installed on the machine, confirm that the following

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

registry key has been created on the machine:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP2\Q296576`

To verify the individual files, use the date/time and version information provided in the following registry key:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP2\Q296576\Filelist`

2. The affected binaries and their associated updated version are:

Name	Version	Name	Version
msw3prt.dll	5.0.2195.3555	adsiis.dll	5.0.2195.3554
infoadmn.dll	5.0.2195.3554	asp.dll	5.0.2195.3554
httpext.dll	0.9.3940.21	httpodbc.dll	5.0.2195.3554
isatq.dll	5.0.2195.3554	ism.dll	5.0.2195.3554
w3svc.dll	5.0.2195.3554	w3ctrs.dll	5.0.2195.3554
ssinc.dll	5.0.2195.3554	Infocom.dll	5.0.2195.3554
fp4Autl.dll	4.0.2.4701	iisrtl.dll	5.0.2195.3554

Note: updates are required in both in the `\%system32%\` and `%system32%\Dllcache` directories,
`C:\Program Files\Common Files\Microsoft Shared\Web Server _ Extensions\40\bin\fp4Autl.dll,`
`%System32%\inetsrv\httpext.dll`
`%System32%\inetsrv\isatq.dll`
3. %System32%\inetsrv\infocomm.dll

4. Disable IPP in Group policy
```
> Launch MMC.exe
> Add/Remove Snap-in and click "Add" in bottom left corner
> Select "Group Policy" Snap-in & Close
> Computer Configuration
> Administrative Templates
> Printers
> Set "web-based printing" to "Disabled"
> Applies when computer is next restarted
```

5. Removing the '.printer' mappings from the IIS websites via the MMC IIS snap-in will **not** disable the service as Group Policy will override this change, and there are reported problems with Exchange Outlook Web Access services.

6. Since Firewalls must be open to TCP connections on Port 80 for normal web traffic, there is little we can do to filter the traffic. Intrusion Detection Systems alerting will keep us informed of requests (legitimate or otherwise) to the service. Update the signatures and rules to the latest versions and manually check for the alert filters. For example:

SNORT rule within "web-iis.rules" should read:
```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS 5
.printer isapi"; flags: A+; content: ".printer"; nocase; reference:
arachnids,533;)
```

and more importantly, the remote shell exploit by Dark Spyrit:
```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS 5
Printer-beavuh"; flags: A+; content: "|33 C0 B0 90 03 D8 8B 03 8B 40
60 33 DB B3 24 03 C3|"; reference:arachnids,535;)
```

Or ISS RealSecure, In user defined events, check for "`null\.printer`" or "`\.printer$`" in "URL_Data", depending upon whether or not the ISAPI filter is known to be installed and implemented.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

2. Microsoft IIS CGI Filename Decode Error Vulnerability

CERT advisory:	CA-2001-12
CVE:	CAN-2001-0333
Microsoft Bulletin:	MS01-026
Initially discovered by:	Network Security Focus Security Team

IIS process requests to execute scripts and perform a URL decoding pass to format the request in it's long canonical form, and applies security checks on the decoded request. A vulnerability results from a second, superfluous decoding pass is performed after the security checks are completed.

The second decoding could enable the request to execute operating system commands or programs outside the virtual folder structure without having the appropriate resource request security checks applied. These would be executed with the context of the `IUSR_machinename` account, which if it remains a member in the `Everyone` group, would grant the attacker similar privileges to a regular system user interactively logged on at the console.

Opening a browser window and typing the following in the address bar
`http://hostname.example.com/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\`

Will return a listing of the contents of the `C:\` drive, as if logged-in interactively at the console. The exploit requires the launch directory to be "`Script Source Access`" enabled in order for the traversal to be effected. The `charmap.exe` tool provided by Microsoft in the O/S is a good way of finding the Unicode for particular characters and symbols if testing requires executing other commands.

Is It Running?
If IIS is running, then the affected component is available to attack, since request string decodes are a key component of implementing RFC 2396 [9] within the web server.

Is It Required?
If IIS is required on the host to provide web server services, this is a key component of IIS and will be required to run the service.

Addressing the Vulnerability

1. Install the Microsoft patch from:
   `http://www.microsoft.com/Windows2000/downloads/critical/q293826/download.asp`. The patch file is called `Q293826_W2K_SP3_x86_en.EXE` under Windows 2000.

   Verify that the patches have been installed on the host:
   To verify that the patch has been installed on the machine, confirm that the following registry key has been created on the machine:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q293826`

   To verify the individual files, use the date/time and version information provided in the following registry key:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q293826\Filelist`

2. Check the DLL binary version. It should be at least or greater than the following:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Binary	Location	File Size	Version Number
Aqueue.dll	%system32%\inetsrv	320,784	5.0.2195.3712
SMTPSVC.DLL	%system32%\inetsrv	434,448	5.0.2195.3779
Ntfsdrv.dll	%system32%\inetsrv	38,160	5.0.2195.3649
Mailmsg.dll	%system32%\inetsrv	66,832	5.0.2195.3712

3. Depending upon your level of paranoia, remove "Script Source Access" property, or remove the virtual server mappings to Scripts directory is not used or required:

```
> Run mmc.exe and Add Internet information Services snap -in
> Expand the tree view to the hostname and the Default Website
> Right click the Scripts directory
> Delete if it is not required
```

4. Separate your IIS web content onto a separate logical disk which would prevent the directory traversal exploit from gaining access to key operating system files (such as cmd.exe in the above example)

5. Review file permissions and command execution for `!USR_hostname` and `Everyone` group with particular access to binaries in `%system32%`. These should be hardened.

3. Remote command execution via Buffer Overflow in Indexing Service

CERT advisory CA-2001-13
CVE CAN-2001-0500
Microsoft Bulletin MS01-033
Initially discovered by: EEye Digital Security

Infamously exploited by the "Code Red" worm that is estimated by Caida.org [[11]] to have successfully infected 359,000 hosts within 14 hours of its initial release. This exploit gives those with access to unpatched servers the ability to execute commands within the SYSTEM context remotely through overflowing the buffer in the IIS ISAPI filter set to listen for ".ida" and ".idq" requests.

Index Server is the built-in search engine in Windows 2000 that catalogues and indexes files and properties of the hard drive. Improper bounds checking on the input buffers on the DLL file (`%system32\idq.dll`) allows additional characters to be forced into the process space, overflowing the buffer and providing memory space for shellcode insertion. As with all buffer overflows, the shell code simply requires to launch and bind a command shell to listen on a specific port and the attacker to connect to the port using netcat or telnet.

Note that all versions of NT4 running IIS 4, Windows 2000 Professional, all versions of Windows 2000 Server and even Windows XP Beta are exposed to the vulnerability.

Is It Running?
The first step is to check Indexing Service is running, since it isn't activated by default. This can be done either by:

```
> run MMC.exe and Add "Services" Snap-in
> Right-click Indexing Service and select "Properties"
> Service status = "Started" and Startup-type of "automatic" or
"manual"
```

or

```
Telnet (nc) host.example.com 80
GET /NULL.ida?[buffer]=x
Host: localhost <return><return>
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Where [buffer] is a string of characters [AAAAAAAA]. This will respond with

```
HTTP 200 OK...
```

The next check to see if it is running is to verify if the binary installed? Check for the installation of `%System32%\cisvc.exe` and when it was last accessed. Check:

```
> Start > Settings > Control Panel > Add/Remove programs
> Select Windows components
> Is Indexing Service installed?
```

Exploring the `C:\System Volume Information\` directory (Note: you may need to add yourself as a user in security properties to view the contents of the hidden directory), combined with the existence of the directory and contents such as `INDEX.00X`, `propstor.bkX` give a clear indication of an active service.

Is it required?

If you are running a web server in a basic manner, it is unlikely that the service is required. However, there are a number of ways of viewing the usage:

Examine the web server log files, which can be found at `c:\winnt\system32\logfiles\w3svc2\exyymmdd.log`

Open the indexing service and look at the number of catalogues defined by:
Executing `c:\winnt\system32\ciadv.msc` MMC plug-in and manually verifying catalogues are being created and indexed.

Search functionality included within the site or application? Does the application provide document management and searching facilities? If so and no third party document management tools are installed, the service will be required.

In a development or test environment, stop the service and walk through the site or application looking for search errors within the ASP pages.

Addressing the Vulnerability

All Windows 2000 server versions Service Pack 2 and less are vulnerable if using the default installation, as well as Windows 2000 Professional workstations and Windows XP Beta IIS 6.0. Addressing the Indexing Service vulnerability requires a number of steps.

1. Apply the Microsoft patch from `http://www.microsoft.com/Windows2000/downloads/critical/q300972/download.asp`. This has a dependency on Service Pack 2 being installed. The patch file is called `Q300972_W2K_SP3_x86_en.exe` under Windows 2000

2. Verify that the patches have been installed on the host:
   To verify that the patch has been installed on the machine, confirm that the following registry key has been created on the machine:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP2\Q300972`

   To verify the individual files, use the date/time and version information provided in the following registry key:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP2\Q300972\Filelist`

3. Check the DLL binary version. It should be at least " 5.0.2195.3645" or greater

Binary	Location	File Size	Version Number
idq.dll	%system32%	121,104	5.0.2195.3645
idq.dll	C:\winnt\system32\DllCache	121,104	5.0.2195.3645

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

4. Download the Microsoft Code Red Cleaning Tool from:
   http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31878

5. Download a Code Red scanner from EEye at
   http://www.eeye.com/advisories/tools/codered.exe , and manually test for false positives and negatives.

6. Remove the ISAPI extension mapping for .ida and .idq

7. Stop the Indexing service running and disable it from starting at boot time

8. Uninstall Indexing Service and remove the components \ if not absolutely necessary

9. Since Firewalls must be open to TCP connections on Port 80 for normal web traffic, there is little we can do to filter the traffic. Intrusion Detection Systems alerting will keep us informed of requests (legitimate or otherwise) to the service. Update the signatures and rules to the latest versions and manually check for the alert filters. For example:

   SNORT rule within "web-iis.rules" should read:
   alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS 5 .printer isapi"; flags: A+; content: ".printer"; nocase; reference: arachnids,533;)

   and more importantly, the remote shell exploit by Dark Spyrit:
   alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS 5 Printer-beavuh"; flags: A+; content: "|33 C0 B0 90 03 D8 8B 03 8B 40 60 33 DB B3 24 03 C3|"; reference:arachnids,535;)

   Or ISS RealSecure, In user defined events, check for "null\.printer" or "\.printer$" in "URL_Data", depending upon whether or not the ISAPI filter is implemented.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

4. SMTP Relaying vulnerability

CERT advisory	N/A
CVE	CAN-2001-0504
Microsoft Bulletin	MS01-037
Initially discovered by:	Joao Gouveia

SMTP is the standard messaging component of Windows Servers, installed by default through Option Pack on NT4 or as part of the Internet Information Services set-up in Windows 2000. It can also be installed as an additional component of Windows 2000 Professional. SMTP mail is the Internet standard for email messaging, defined through standards such as RFC 2821 [19]. SMTP is implemented as a stand-alone service within Windows 2000, and is physically separate from the Exchange Server implementation of SMTP.

The vulnerability extends from an authentication error in the service. The server accepts incorrect authentication information and authorises access to the resources. The scope of this vulnerability would permit only user level access to the system – i.e. send mail from the server with all the servers' valid header and I.P addresses. The scope of this vulnerability is also confined only to standalone Windows 2000 servers, with no domain membership or participation. Servers within a domain structure are not vulnerable. However, this exploit must be addresses as serious, since most Windows 2000 that run IIS are not configured to be part of a domain, and will therefore be vulnerable to this exploit.

This technique is often used to send Spam or potentially damaging or illicit email, and is one of the widest unauthorised uses of computer systems on the Internet. Email will be confirmed as being sent by your organisation, whatever the content. This usually annoys the recipient and solicits an angry response, depending upon the content and offensive nature of the message sent.

Is It Running?

Firstly, confirm the SMTP service is running on the current host, since it is automatically started by default when installed. This can be done either by:

`Run MMC.exe` and add `Services Snap-in`
`Right-click Indexing Service` and select `Properties`
Check whether the `Service status = Started` and `Start-up` type of `Automatic or Manual`

Next identify if the host is establishing connections to the SMTP port. If local access is available to be the server, open a command prompt and type:

```
netstat -an
```

And search the output for Port 25 connections, such as:

```
TCP    0.0.0.0:25    0.0.0.0:0     Listening
```

If no access is available to a host console to run the `netstat` command, then use a port scanner (FScan, NMapNT, Superscan, ISS etc.) to identify the port as openly available from within the firewall. The result should be a connection to the host available on Port 25.

The next test to try is try to establish a manual connection to the port and verify it is the Microsoft SMTP service configured and listening, and that any SMTP server connections are not provided by a 3rd party. To do this, type:

```
Telnet (or nc) host.example.com 25
```

The output should provide the following banner responses if Microsoft IIS SMTP:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
220 host Microsoft ESMTP MAIL Service, Version: 5.0.2195.1600 ready
```

While you are there, test the authentication of the service:

```
Telnet (or nc) host.example.com 25   (or continue the above session)
HELO
MAIL FROM: <mail domain or server hostname>
RCPT TO: postmaster@ hostname
DATA
TO: <users display name>
SUBJECT: Test SMTP message
<CRLF><CRLF>
This is a test message
<CRLF>.<CRLF>
QUIT
```

And view the response.

Is It Required?

It is usual to assume that if SMTP services are installed and running that the service is required. It is wise to gather information about what activity the service is performing, and in what way it is configured.

> Run `mmc.exe`
> Add Snap-In called `Internet Information Services`
> Expand out the explorer, open the tree under the computer name
> Right-click `Default SMTP Virtual Server`
> In the context menu, select `Properties`
> Step through the tab and note the configuration

Be sure to check all webs and virtual directories for the occurrence of SMTP scripts within ASP's. Using the built-in search tool in Windows 2000, we can do string matching:

> `Start > Search >'For Files or Folders'`
> In the left hand search pane, Click into the text box labelled `Containing Text`
> Type `CDONTS`
> In the `Look in` drop-down menu, select `Browse`
> `Open the resulting Search Returns, and for each of the ASP pages,`
> Establish whether the string `Server.CreateObject("CDONTS.NewMail")` exists

In anything other than sample code scripts, this is a clear indication that the web sites on that server are interacting using SMTP mail services.

Again, review the IIS log files (`%system32%\LogFiles\SmtpSvc1\ex`*`yymmdd`*`.log and archived logs`) either manually reading the logs, by opening the log file in notepad or using a log analyser such as Webtrends. Check the last log entry for date and time stamp for recent use, and establish how frequently the service is used – the total connections for that log cycle.

Addressing the Vulnerability

All Windows 2000 server versions Service Pack 2 and less are vulnerable if using the default installation, as well as Windows 2000 Professional workstations and Windows XP Beta IIS 6.0. Addressing the Indexing Service vulnerability requires a number of steps.

1. Apply the Microsoft patch from `http://www.microsoft.com/Windows2000/downloads/critical/q302755/download.asp.` This has a dependency on Service Pack 2 being installed. The patch file is called `Q302755_W2k_SP3_x86_en.exe` under Windows 2000.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

2. Verify that the patches have been installed on the host:
   To verify that the patch has been installed on the machine, confirm that the following registry key has been created on the machine:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows2000\SP3\Q302755`

3. To verify the individual files, use the date/time and version information provided in the following registry key:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows2000\SP3\Q302755\Filelist`

4. Check the DLL binary version. It should be at least or greater than the following.

Binary	Location	File Size	Version Number
smtpsvc.dll	%system32%\inetsrv	434,448	5.0.2195.3779
ntfsdrv.dll	%system32%\inetsrv	38,160	5.0.2195.3649
mailmsg.dll	%system32%\inetsrv	66,832	5.0.2195.3712
aqueue.dll	%system32%\inetsrv	320,784	5.0.2195.3712

5. If the service is not required, stop the SMTP service running and disable it from starting at boot time using the services plug-in for the MMC. If the SMTP feature is permanently not required, uninstall the SMTP Service and delete the components from the system.

6. Firewalls are invariably open to TCP connections on Port 25 for normal web messaging when the service is required. If the service is not required on the host, a firewall would very effectively block communication attempts to the SMTP service. Intrusion Detection Systems alerting will keep us informed of requests (legitimate or otherwise) to attempted usage of the service. Update the signatures and rules to the latest versions and manually check for the alert filters.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

5. Buffer Overflow in FrontPage server extension (MS-01-035)

CERT advisory	N/A
CVE	CAN-2001-0341
0Microsoft Bulletin	MS01-035
Initially discovered by:	Network Security Focus (NSFOCUS)

FrontPage extensions ship with IIS4 and IIS5, Office 2000 and Office XP, and extend the functionality of the IIS web server to support components used in the Visual Studio development suite. One optional feature of the FrontPage extensions is Visual Studio RAD component, installed from the Windows 2000 CD, which contains an unchecked buffer vulnerability. The VS RAD feature allows developers to deploy custom COM components by allowing authenticated authors to upload COM components onto the server.

The unchecked buffer in the request processing routine allows a malformed command to insert shellcode into the FrontPage process space, yielding access at either `IUSR_<hostname>` or system-level privileges. The buffer overflow occurs if `fp30reg.dll` receives a URL request that is longer than 258 bytes, exposed through a lack of length checking on the input string. Exploiting this vulnerability successfully, an attacker can obtain the privilege of `IUSR_<hostname>` account (unprivileged user) in IIS 5.0 or Local System account when performing a combination of attacks to elevate privileges.

Visual Studio RAD component is not selected by default in the installation options, as is actively alerted as not suitable for production systems during installation if selected. The two key issues are that production servers do not development and test service installed, and that development and UAT servers as most at risk to this flaw, and are commonly attached to the public network.

Is It Running?

1. Establish whether the components are installed. This is done by typing:

   > Start > Settings > Control Panel > Add/Remove Programs
   > Select "Add/Remove Windows components"
   > Select IIS
   > Scroll down and note whether "Visual Studio RAD Remote Deployment Support" is selected

   Check the IIS directories for the existence of the publishing files. Telnet or Netcat to the service:

   ```
   nc host.example.com 80
   GET /_vti_bin/_vti_aut/fp30reg.dll?[Ax258] HTTP/1.1
   Host: localhost
   ```

2. Compile and run the proof-of-concept exploit written by NSFOCUS, available at `http://www.nsfocus.com/proof/fpse2000ex.c` .

Is It Required?

Is the server being examined a production or development / test host? Microsoft strongly advises against installing the VS RAD deployment support on production hosts, due to the serious threat of 3rd parties installing unauthorised COM components onto the server.

If the host is a development or test box, you should enquire whether the feature is being used by the development teams, explain the risks, and request the features to be removed. Internal servers are just as at risk as production boxes to vulnerabilities.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Addressing The Vulnerability

1. Uninstall the Visual Studio RAD components from Production Servers, or

2. Apply the Microsoft patch from `http://www.microsoft.com/downloads/release.asp?releaseid=30727`. This has a dependency on Service Pack 2 being installed. The patch file is called `Q300477_W2K_SP3_x86_en.EXE` under Windows 2000

3. Verify that the patches have been installed on the host:
   To verify that the patch has been installed on the machine, confirm that the following registry key has been created on the machine:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q300477`

   To verify the individual files, use the date/time and version information provided in the following registry key:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q300477\Filelist`

4. Check the binary versions of FrontPage components from the following table:

Binary	Location	File Size	Version Number
FP30REG.DLL	\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\ISAPI_vti_auth	94,308	4.0.2.5121
FP4AREG.DLL	\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\bin	94,308	4.0.2.5121
FP30MSFT.DLL	\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\servsup	176,186	4.0.2.5322
FP4AWEL.DEL	\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\bin	852,023	4.0.2.5322

5. Install an application-level firewall such as Entercept Web Server Edition, EEye Secure IIS or such others. These products are created specifically with intercepting suspicious looking buffers and string aimed at ISPAI extensions and other DLL exposures.

References

1. Davis, John, "From Blueprint to Fortress: A Guide to Securing IIS 5.0" `http://www.microsoft.com/TechNet/prodtechnol/iis/deploy/depovg/securiis.asp`, June 2001

2. Howard, Michael, "Secure Internet Information Services 5.0 Checklist", `http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/iis5chk.asp`, 6/29/2001

3. Microsoft Corporation, "Microsoft Network Security Hotfix Checker is available", `http://support.microsoft.com/support/kb/articles/q303/2 /15.asp?id=303215&sd=tech`, 8/15/2001

4. Microsoft Corporation, hfnetchk.exe tool, `http://www.microsoft.com/technet/itsolutions/security/tools/hfnetchk.asp`, 8/15/01

5. RFC2396
   Internet Engineering Task Force, "Internet Printing Protocol", `http://www.ietf.org/rfc/rfc2396.txt`, August 1998

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

6. EEye Security Inc, “Windows 2000 IIS 5.0 Remote buffer overflow vulnerability” http://www.eeye.com/html/Research/Advisories/AD20010501.html , 1/5/2001

7. Security Focus, “Microsoft Windows 2000 IIS 5.0 IPP ISAPI 'Host:' Buffer Overflow Vulnerability”, http://www.securityfocus.com/frames/?content=/vdb/%3Fid%3D2674 , 05/01/01

8. RFC 2396
Internet Engineering Task Force, “Uniform Resource Identifiers (URI): Generic Syntax “, http://www.ietf.org/rfc/rfc2396.txt , August 1998

9. Security Focus, “NSFOCUS Security Advisory (SA2001-02)”, http://www.nsfocus.com/english/homepage/sa01-02.htm, 15/6/2001

10. Security Focus, “MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability”, http://www.securityfocus.com/bid/2708 , 5/15, 2001

11. Caida.org, “CAIDA Analysis of Code-Red”, http://www.caida.org/analysis/security/code-red/, August 2001

12. SecuriTeam, “Unchecked Buffer in Index Server ISAPI Extension Leads to Web Server Compromise”, http://www.securiteam.com/windowsntfocus/5FP0B2K4KU.html , 6/19/2001

13. SecuriTeam, “Exploit Code Released for the Index Server ISAPI Extension Vulnerability (IDQ)”, http://www.securiteam.com/exploits/5HP0N2A4KQ.html , 28/6/2001, 6/28/2001

14. EEye Security Inc, “All versions of Microsoft Internet Information Services Remote buffer overflow”, http://www.eeye.com/html/Research/Advisories/AD20010618.html , 6/18/2001

15. EEye Security Inc, “.ida "Code Red" Worm”, http://www.eeye.com/html/Research/Advisories/AL20010717.html , 7/17/2001

16. SANS Incidents.org, “Code Red Threat FAQ”, http://www.incidents.org/react/code_red.php , 5/8/2001

17. EEye Security Inc, “Code Red II Worm Analysis”, http://www.eeye.com/html/Research/Advisories/AL20010804.html , 4/8/2001

18. SANS Incidents.org, “Code Red II Worm Analysis”, http://www.incidents.org/react/code_redII.php, 7/8/2001, 4/8/2001

19. RFC 2821
Internet Engineering Task Force, ” Simple Mail Transfer Protocol”, http://www.ietf.org/rfc/rfc2821.txt , April 2001.

20. Network Security Focus, “Microsoft FrontPage 2000 Server Extensions Buffer Overflow Vulnerability”, http://www.nsfocus.com/english/homepage/sa01-03.htm, 6/25/01

21. NSFOCUS, “Proof of concept code for fp30reg.dll overflow bug” http://www.nsfocus.com/proof/fpse2000ex.c , 2001

22. SecurityFocus.com, “MS Visual Studio RAD Support Buffer Overflow Vulnerability”, http://www.securityfocus.com/bid/2906 , 6/21/2001

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

23. Chaddock, Mary, “A Breakdow n of the SANS Top Ten Threats”, October 11, 2000, http://www.sans.org/infosecFAQ/threats/top_ten.htm

24. Bys, Corey, “Securing Windows 2000 Server”, May 20, 2001, http://www.sans.org /infosecFAQ/win2000/sec_server.htm

© SANS Institute 2001, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**