

Re: Microsoft Warns of New Windows Flaw (March 19, 2003)

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-07/1626.html>

From: Larry (*nospam_at_home.com*)

Date: 07/30/03

Date: Wed, 30 Jul 2003 01:21:06 GMT

It's fairly easy to seal up Win98SE.

In WINDOWS SETUP in ADD/REMOVE PROGRAMS of Control Panel

Uninstall Windows Scripting Host that runs .vbs scripts (no OS, no LoveLetter) This is located inside "ACCESSORIES".

Make sure IE "INTERNET TOOLS" are all uninstalled.

Make sure ONLINE SERVICES are all uninstalled unless you're actually forced to use one of them...yecch....AOL.

Uninstall Outlook Express (and Outlook), the biggest cracker target every devised. Running it is like walking around with a big red target on a t-shirt that says "KILL THIS AMERICAN" in Baghdad. Why run software that's the TARGET when there are untargetable or not-targeted softwares that work better like Pegasus 4 for email and Free Agent for newsgroups, which are NOT connected to the IE spammer automatically? How silly..... Xnews, like the other two, is FREE and works MUCH better for binaries.

Before uninstalling Outlook, you might want to save your ADDRESS BOOK to paper so you can put it in your new email program that ISN'T used by every email worm on the net. Delete all ADDRESS BOOK entries then ADDRESS BOOK before uninstalling Outlook because I think this worm source stays installed as a remnant for the wormers to use.

Run two browsers....One for general browsing of unknown sites that has Java, Javascript, ActiveX and all the other script runner toys Billy built for the spammers turned off. Seal it up tight so it will only BROWSE sites that will run without all the crapware installs.

Leave IE wide open, but ONLY use it for websites you MUST have open browsing for, like windowsupdate.microsoft.com to get the latest patches. NEVER browse other sites with it.

Install WebWasher the spammers are terrified of free from

www.webwasher.com. Thank the genius engineers from Siemens in Germany for inventing it. No popup windows, referrers dragging you off to some spammer to be screwed, no moving GIF ads blinking and playing spam for you, and it adds another layer of protection from cookies, web bugs, javascripts and other crapware. You can even go to a Geocities website without a single popup in front of you to spoil the view. Some sites won't work. If you HAVE to have it, just click WW's blue icon in the tray and a red X comes up and it's totally bypassed so you can be TRASHED in the usual way. Turn it off before going to Windows Update, too!

Install StartUpMonitor from Mike Lin for free from:

<http://www.mlin.net/StartupMonitor.shtml>

This little transparent program runs way in background and simply prevents EVEN MICROSOFT from installing ANYTHING in the RUN key of the Registry that will boot when Windoze starts up. It will drive you crazy when you run Windows Update (just keep saying OK) but is really neat when it pops up asking you if some spammer or spyware operator can install his spyware in your computer at the oddest times while browsing or installing new software. THEN SAY NO! Paypal Mike a little tip for saving your ass with such neat stuff. Not even Microsoft gets by it!

Uninstall another sinister Spammer....anything Macromedia codes....Flash, etc. To shed yourself of it, you'll have to tell Webwasher to NEVER GO to Macromedia for the automatic installs of this crapware in lots of webpages. Flash was compromised long ago by some clever crackers. Go to www.securityfocus.com and put Macromedia into the search box. There are 89 current vulnerabilities for you to read. You don't need it....You didn't want it....You can live without anything Macromedia writes and the spammers use to play you a movie on their clever webpage while they install the spyware and spycookies. You'll need to edit your Registry to clean Macromedia products out of it. There are HUNDREDS of keys in your registry installed by Flash to delete. Webwasher WILL prevent webpages from sending you off to Macromedia for a fresh download of Flash when they don't find it to run. Not having Javascript running also prevents its unwanted re-installation.

If you are a single user internet user, not networking your computer with any others or printers or a LAN, then the ONLY "device" you need to access the internet is TCP/IP for either your dialup adapter if you're a dialup kinda guy or TCP/IP for your Ethernet adapter if you have cable or DSL. DSL customers may also need PPPoE, a kind of dialup for DSL users to unload the system they lied to you about having a 24/7 connection, which you don't.

Open NETWORK on Control Panel (or its new hidden equivalent on XP, it's own problem stack). Look at the components installed. There are only TWO installed in any independent system I install. The adapter for either the dialup modem or Ethernet adapter is one. If you use

your USB port to connect up to broadband, you need an Ethernet card. The other is TCP/IP protocol for THAT adapter ONLY. Unless you network with other computer in your LAN, you don't need or desire ANY OTHER COMPONENT....like Microsoft Networking, NetBIOS, NetBEUI and all that other networking crap the kiddie crackers use to trash your system. REMOVE them. There, now your 137 port is NOT listening, nor are the others. TCP/IP will let you talk to everything on the net and it works great!

Even if you never want to buy a second computer for the kids, buy a Netgear \$69 router from your fav computer outlet. Its NAT takes your whole computer OFF THE INTERNET so the kiddie crackers can't get to it. Your address exposed to Windoze and any software reading it is USELESS to "them". Mine is 192.168.0.2 on this machine. Go ahead and attack it. Your real IP is NOT in the computer, its software, spyware or trojans. The router translates your internet IP to this one, and loads your computer with everything it needs to connect, automatically if you have your computer setup to automatically get IP. The router is like your own little internet provider. The router also, by default, doesn't ping, answer connect requests, leave ports open you're not using like Windoze does, and the BEST thing is it GETS YOUR SWISS CHEEZE WINDOZE OPERATING SYSTEM AWAY FROM THE CRACKERS who know how to trash it. It's so cheap and SO SIMPLE. Now you can even uninstall all the bogus software firewalls sucking up all your computer's CPU time running UNDER the OS's vulnerabilities. Pick any "security test" site.....You'll be in full stealth mode unless YOU tell the router, otherwise....like my PORTS entry so my friends can get to my FTP server on one of my computers.

Here's my current NETSTAT -an:

```
C:\WINDOWS>netstat -an
```

Active Connections

```
Proto Local Address Foreign Address State
TCP 0.0.0.0:1128 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1513 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1030 0.0.0.0:0 LISTENING
TCP 127.0.0.1:8081 0.0.0.0:0 LISTENING
TCP 192.168.0.2:21 0.0.0.0:0 LISTENING
TCP 192.168.0.2:1128 216.168.3.44:119 ESTABLISHED
TCP 192.168.0.2:1513 63.223.5.254:119 ESTABLISHED
```

```
C:\WINDOWS>
```

The bottom two entries and the top two entries are two connections to two usenet servers I'm currently using to download binaries and the connection for this message. port 8081 is Webwasher waiting for me to browse with Opera 7, my favorite browser. Port 21 is my FTP server waiting for a call. Port 1030 is a port Windoze left open after I called for a SecurityFocus.com webpage for this message.

All those ports, like NetBIOS, are never open because they are NOT INSTALLED!

BUY a good antivirus program, not the AV + firewall you don't need. I recommend a CURRENT PAID SUBSCRIPTION to Norton Antivirus' latest version. The money you send them pays the huge staff that spends so much time keeping the latest vicious bastards out of your computer. FREE antivirus programs aren't worth a damn because the threats are CONSTANTLY changing! No, I don't work for Symantec.

I have a large collection of worms, virii, trojans and spammer scripts, great fun dissecting to see how these demented geniuses do it. Shhh....don't tell Norton AV 2003 or it'll snatch them!

Well, that all works great, here. Symantec occasionally snatches a worm I don't have from my email before I can save it. I'll get more to read...(c;

On Thu, 20 Mar 2003 16:36:25 GMT, The Other Guy <nospam@this.addy> wrote:

>
><http://www.eweek.com/article2/0.3959,941455.00.asp>
>March 19, 2003
>Microsoft Warns of New Windows Flaw
>
>Microsoft Corp. has released a patch for a critical vulnerability in
>every version of Windows from 98 forward.
>The flaw lies in the Windows Script Engine for Jscript, which enables
>the operating system to execute script code. The engine incorrectly
>processes the script and does not correctly size a buffer during a
>memory operation. As a result, an attacker could cause a buffer
>overflow and execute code of his choice on a vulnerable machine.
>
>In order to exploit this problem, the attacker would either need to
>construct a Web page that contains the malicious code and lure a user
>to the page or send the user an HTML mail message with the code
>included.
>
>Any code the attacker is able to execute on the user's machine would
>run with the user's privileges.
>
>This vulnerability affects Windows 98, 98 SE, Me, NT 4.0, NT 4.0
>Terminal Server Edition, 2000 and XP. However, there are several
>mitigating factors that could prevent exploitation of the flaw. Users
>who have disabled active scripting in Internet Explorer would not be
>vulnerable to either of the above attacks. Also, Outlook Express 6.0
>and 2002 block the automatic execution of the HTML mail attack, as do
>Outlook 98 and 2000 when the Outlook Email Security Update is
>installed.
>

comp.security.firewalls: Re: Microsoft Warns of New Windows Flaw (March 19, 2003)

>patch site:

>*Flaw in Windows Script Engine Could Allow Code Execution*

><http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-008.asp>

>

>

>---

>./configure --prefix=~/.zyterion

>*Not this guy or that guy, The Other Guy.*

>

>*This spot may contain a satirical comment or comedic source,*

>*and is meant to be funny. If you are easily offended, gullible*

>*or don't have a sense of humour we suggest you read elsewhere.*

Larry W4CSC

"No, NO, Mr Spock! I said beam me down a WRENCH,
not a WENCH! KIRK OUT!"