

Re: !!Windows Is Infected!!

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-04/8796.html>

From: Bruce Chambers (*bchambers_at_nospamcableone.net*)

Date: 04/09/04

Date: Fri, 9 Apr 2004 08:59:03 -0600

Greetings --

These messages are not caused by a Trojan or other infection; they're originating outside the very unsecure PCs. They're from a very unscrupulous "business." It's a scam, plain and simple. They're trying to sell you patches that Microsoft provides free-of-charge. They're also demonstrating that your PC is very unsecure.

Does the title bar of these pop-ups not read "Messenger Service?"

This type of spam has become quite common over the past year or so, and unintentionally serves as a valid security "alert." It demonstrates that you haven't been taking sufficient precautions while connected to the Internet. Your data probably hasn't been compromised by these specific advertisements, but if you're open to this exploit, you most definitely open to other threats, such as the Blaster Worm that still haunts the Internet. Install and use a decent, properly configured firewall. (Merely disabling the messenger service, as some people recommend, only hides the symptom, and does little or nothing to truly secure your machine.) And ignoring or just "putting up with" the security gap represented by these messages is particularly foolish.

Messenger Service of Windows

<http://support.microsoft.com/default.aspx?scid=KB;en-us;168893>

Messenger Service Window That Contains an Internet Advertisement Appears

<http://support.microsoft.com/?id=330904>

Stopping Advertisements with Messenger Service Titles

<http://www.microsoft.com/windowsxp/pro/using/howto/communicate/stopspam.asp>

Blocking Ads, Parasites, and Hijackers with a Hosts File

<http://www.mvps.org/winhelp2002/hosts.htm>

microsoft.public.windowsxp.general: Re: !!Windows Is Infected!!

Whichever firewall you decide upon, be sure to ensure UDP ports 135, 137, and 138 and TCP ports 135, 139, and 445 are all blocked. You may also disable Inbound NetBIOS (NetBIOS over TCP/IP). You'll have to follow the instructions from firewall's manufacturer for the specific steps.

You can test your firewall at:

Symantec Security Check

http://security.symantec.com/ssc/vr_main.asp?langid=ie&venid=sym&plfid=23&pkj=GPVHGBYNCJEIMXOKCDT

Security Scan – Sygate Online Services

<http://www.sygatetech.com/>

Oh, and be especially wary of people who advise you to do nothing more than disable the messenger service. Disabling the messenger service, by itself, is a "head in the sand" approach to computer security. The real problem is not the messenger service pop-ups; they're actually providing a useful, if annoying, service by acting as a security alert. The true problem is the unsecured computer, and you've been advised to merely turn off the warnings. How is this helpful?

Bruce Chambers

--

Help us help you:

<http://dts-l.org/goodpost.htm>

<http://www.catb.org/~esr/faqs/smart-questions.html>

You can have peace. Or you can have freedom. Don't ever count on having both at once. -- RAH

"phil" <locutus5000511@hotmail.com> wrote in message

news:1a78301c41e31\$9ee6c090\$a501280a@phx.gbl...

i keep getting an error message that pops up in the background that closes everything i am doing something has gotten into windows messenger service causing the popup on me then it says theres a cure for it and ask me to go to this site <http://www.windows-patch.info/> which i believe its a fake microsoft site the patch links on the site ask for money so if anyone knows what this problem is can you e-mail me

Windows@Patch.info

This Security Fix is compatible with the following

Microsoft® Windows® Systems:

Microsoft Windows XP

Microsoft Windows NT Workstation

Microsoft Windows NT

Microsoft Windows 2000

Microsoft Windows Server 2003

Microsoft Security Bulletin MS03-043

Buffer Overrun in Messenger Service Could Allow Code Execution (828035)

Issued: October 22, 2003

Version Number: 1.1

Summary

Who Should Read This Document: Customers using Microsoft® Windows®

Re: !!Windows Is Infected!!

microsoft.public.windowsxp.general: Re: !!Windows Is Infected!!

Impact of Vulnerability: Remote Code Execution
Maximum Severity Rating: Critical
Recommendation: Microsoft® Windows® should install a patch immediately
Caveats: None
Tested Software and Patch Download Locations:
Affected Software:
Microsoft Windows NT Workstation - Download a fix to patch this issue
Microsoft Windows NT - Download a fix to patch this issue
Microsoft Windows 2000 - Download a fix to patch this issue
Microsoft Windows XP - Download a fix to patch this issue
Microsoft Windows Win98 - Download a fix to patch this issue
Microsoft Windows Server 2003 - Download a fix to patch this issue
Non Affected Software:
Microsoft Windows Millennium Edition
The software listed above has been tested to determine if the versions are affected. Other versions are no longer supported, and may or may not be affected.
Technical Description:
A security vulnerability exists in the Microsoft® Messenger Service that could allow arbitrary code execution on an affected system. The vulnerability results because the Messenger Service does not properly validate the length of a message before passing it to the allocated buffer.
An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause the Messenger Service to fail. The attacker could then take any action on the system, including installing programs, viewing, changing or deleting data, or creating new accounts with full privileges.
Mitigating factors:
Messages are delivered to the Messenger service via NetBIOS or RPC. If users have blocked the NetBIOS ports (ports 137-139) - and UDP broadcast packets using a firewall, others will not be able to send messages to them on those ports. Most firewalls, including Internet Connection Firewall in Windows XP, block NetBIOS by default.
Disabling the Messenger Service will prevent the possibility of attack.
On Windows Server 2003 systems, the Messenger Service is disabled by default.
Severity Rating:
Windows NT Critical
Windows Server NT 4.0 Terminal Server Edition Critical
Windows 2000 Critical
Windows XP Critical
Windows Server 2003 Moderate
The above assessment is based on the types of systems affected by the vulnerability, their typical deployment patterns, and the effect that exploiting the vulnerability would have on them.

Re: !!Windows Is Infected!!