

Re: Virus in microsoft Patch

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-08/7220.html

From: JoshV (marksto_at_microsoft.com)

Date: 08/20/03

Date: Tue, 19 Aug 2003 19:23:46 -0700

Here is a more complete solution:

You have probably received the following error messages when using your computer:

"This system is shutting down. Please save all work in progress and log off. This shutdown was initiated by NT Authority/System."

"Windows must restart because the Remote Procedure Call (RPC) service terminated unexpectedly."

This is a known security issue which was first found on July 15. There is currently an Internet Worm that is taking advantage of this security issue. Microsoft published the patch to fix this issue on July 16 for all of the affected systems on our web site. For more information, please refer to the following page:

Microsoft's latest Information on the Blaster Worm including links for other Windows Operating Systems
<http://www.microsoft.com/security/incident/blast.asp>

For the latest information on this security bulletin
http://www.microsoft.com/security/security_bulletins/ms03-026.asp

The resolution to this issue is to clean the worm from your system and install the patch mentioned above.

Do this In Order:

- 1) Turn on your Internet Connection Firewall (Windows XP)
- 2) Install the patch from Microsoft to remove the vulnerability

- 3) Run a removal Tool from an Anti-Virus company to remove all traces of the virus from your system
- 4) Go to Windows Update and get all other needed Critical Updates

Alternate Download Sites are located at:

 <http://www.microsoft.com/downloads/details.aspx?FamilyID=2354406c-c5b6-44ac-9532-3de40f69c074&displaylang=en>

http://download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/WindowsXP-KB823980-x86-ENU_1d296adab6699e66210e5a350236381.exe

IMPORTANT

Whenever your computer attempts to shutdown or reboot, quickly:
Click the Start Button and then click RUN and type in shutdown -a and hit enter.
This should halt the rebooting problem temporarily.

You can also disconnect your computer from the internet while you do the first step of turning on the Internet Connection Firewall.

1)
Turn on the Internet Connection Firewall (Windows XP)
For XP Pro Users
<http://www.microsoft.com/windowsxp/pro/using/howto/networking/icf.asp>

For XP Home Users
<http://www.microsoft.com/WindowsXP/home/using/howto/homene/t/icf.asp>

Generic Instructions for XP Users:

1. In Control Panel, double-click "Networking and Internet Connections", and then click Network Connections.
2. Right-click the connection (your internet connection) on which you would like to enable ICF, and then click Properties.
3. On the Advanced tab, click the box to select the option to "Protect my computer or network".
4. If you want to enable the use of some applications and services through the firewall, you need to enable them by clicking the Settings button, and then selecting the programs, protocols, and services to be enabled for the

ICF configuration.

2)

Install the Patch from Microsoft for your Operating System
Windows XP (32-bit)

<http://download.microsoft.com/download/9/8/b/98bcfad8-afbc-458f-aaee-b7a52a983f01/WindowsXP-KB823980-x86-ENU.exe>

3)

Run a removal Tool from an Anti-Virus Company to get the
Virus off your system

Network Associates

<http://vil.nai.com/vil/stinger/>

Trend Micro

<http://housecall.trendmicro.com/>

Symantec

<http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html>

Computer Associates

<http://www3.ca.com/virusinfo/virus.aspx?ID=36265>

4)

When you get a chance after everything calms down, with
Internet Explorer up and running, go to the top menu and
click Tools and click Windows Update and install all the
latest Critical Updates.

<http://v4.windowsupdate.microsoft.com/en/default.asp>

You can also configure Automatic Updates to automatically
download updates for you. How to Configure and Use
Automatic Updates in Windows XP:

<http://support.microsoft.com/default.aspx?scid=kb:en-us;306525>

Please note I cannot respond to e-mailed questions.

Please use respond to this thread to let me know if the
steps and suggestions helped you to resolve the issue.

Disclaimer:

This posting is provided "AS IS" with no warranties, and
confers no
rights.

>-----Original Message-----

>Alan;

>You already had the virus (worm).

>That is what was causing your issue.

>Now you can blame Microsoft for your troubles or you can

install the

>patch (should have been done a while ago).

>Enable firewall (why wasn't it enabled)

>

>Follow this carefully to fix the computer:

>You most likely have a worm W32.Blaster.Worm

>DISCONNECT the subject computer from any network
IMMEDIATELY.

>

>Install or enable a firewall IMMEDIATELY:

><http://support.microsoft.com/?kbid=283673>

>

>VERY IMPORTANT to repair, closing ports is NOT enough.

>Download the appropriate patch referenced in Ron
Martessl article

>below.

>You may need to do this at an uninfected computer and
burn to CD or

>save on floppy.

>

>This is the IMPORTANT fix by Ron Martell:

><http://www.bigblackglasses.com/Article.aspx?Article=342>

>

>Also see:

><http://isc.sans.org/diary.html?date=2003-08-11>

>

>After this is resolved prevent similar occurrences by
installing ALL

>Critical Updates from Windows Update.

>Keep antivirus up to date and run at least weekly.

>Install or enable a firewall.

>

>--

>Jupiter Jones [MVP]

>An easier way to read newsgroup messages:

><http://www.microsoft.com/windowsxp/pro/using/newsgroups/s>

etup.asp

><http://dts-l.org/index.html>

>

>

>"Alan" <akendall83@hotmail.com> wrote in message

>news:0d6801c360c6\$df700f00\$a301280a@phx.gbl...

>> Last night I was having problems with the RPC shutting

>> down my computer automatically if I connected to the
net,

>> having phoned my ISP I was directed to a patch on the

>> microsoft website. Upon installing this patch I was

>> informed by my antivirus software that I had

contracted a

>> virus from this patch. So be warned, dont assume

microsoft

microsoft.public.windowsxp.security_admin: Re: Virus in microsoft Patch

>> *files are clean.*

>

>

>.

>