

## RE: Blaster Worm Solution

**Source:**

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2003-08/3571.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-08/3571.html)

---

**From:** Curtis Koenig [MSFT] ([ckoenig\\_at\\_online.microsoft.com](mailto:ckoenig_at_online.microsoft.com))

**Date:** 08/13/03

Date: Wed, 13 Aug 2003 16:37:22 GMT

Hi Nick,

We also recommend the following steps to get started:

1. Remove the infected computer from the network and reboot into Safe Mode.
2. Locate the files below, plus the Value "windows auto update" under the Run registry key and deleted them all:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

MSBLAST.EXE under the "C:\Windows\system32" folder

MSBLAST.EXE-1c3a3376.PIF under the "C:\Windows\prefetch" folder

2a. If you are running Windows XP (any version) it is also recommended that the Internet Connection Firewall be enabled to prevent re-infection when connecting to the internet.

3. Contact your Antivirus provider for assistance in using any removal tools they are providing or you can use one that Symantec is providing. Symantec's Removal tool

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

4. If the OS continues to shut down when trying to connect to <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>, with the dialog box stating the OS will be shutting down in 30 seconds.

Set the RPC Service to "Take No Action" and reboot, this should allow you to download the patch and install it.

--

Curtis Koenig  
Support Professional  
Microsoft Clustering Technologies Support  
MCSA, MCSAS, MCSE, MCSES

This posting is provided "AS IS" with no warranties and confers no rights. Please reply to the newsgroup so that others may benefit. Thanks!

RE: Blaster Worm Solution

microsoft.public.windowsxp.security\_admin: RE: Blaster Worm Solution

-----  
>Sender: "Nick Shtangey" <neo013x@msn.com>  
>Subject: Blaster Worm Solution  
>Date: Wed, 13 Aug 2003 07:41:18 -0700  
>  
>The patch is available at:  
>  
>[http://microsoft.com/downloads/details.aspx?](http://microsoft.com/downloads/details.aspx?FamilyId=2354406C-C5B6-44AC-9532-3DE40F69C074&displaylang=en)  
>FamilyId=2354406C-C5B6-44AC-9532-  
>3DE40F69C074&displaylang=en  
>(This is the 32-bit version. If it does not work, try the  
>64-bit version - search for Blaster Worm)  
>  
>If you cannot stay online long enough to download the  
>patch, try the following.  
>  
>1. When you are informed of the system shutdown,  
> press 'Start' > 'Run' (if you do not see run, you can  
> just press 'Start' and 'R')  
>  
>2. Type in:  
> shutdown -a  
> This uses a built-in Windows utility to abort the  
> shutdown.  
>  
>3. Though this will stop the shutdown, the RPC server has  
> still crashed. This means that you won't be able to do  
> certain things, like access some websites, use  
> cut/copy/paste.  
>  
>4. If you cannot possible download the patch without it,  
> you may try to restart it. But remember that it doesn't  
> always work, and if you make a mistake, it can crash  
> your computer... Then again, what do you have to lose?  
> ;)  
>  
>RESTARTING THE RPC SERVER  
>  
>1. Open 'Control Panel'  
>2. From there, open 'Administrative Tools'  
>3. Select and open 'Services'  
>4. If your RPC server is really down, you will not see  
> anything. Do not panic. At the bottom of the window,  
> you will notice two tabs: 'Extended' and 'Standard'.  
>5. Click on 'Standard'  
>6. You will see a list of Windows System Services. Find:  
> Remote Procedure Call (RPC)  
>7. Double click on it, or right click and  
> select 'Properties'  
>8. Press 'Start'.  
>  
>The service should now start up. If it doesn't, you  
>can restart the computer and try again.  
>  
>For more information/assistance/support, you can email me  
>at neo013x@msn.com or support@neo013.net.  
>  
>Good luck,  
>  
>  
>Nick Shtangey  
>

microsoft.public.windowsxp.security\_admin: RE: Blaster Worm Solution

>P.S. I actually has the virus and have successfully  
>removed it without using the Microsoft patch.  
>