

## Re: 8/11/03 virus

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-08/1628.html>

---

**From:** Pavan ([pavan2\\_at\\_hotmail.com](mailto:pavan2_at_hotmail.com))

**Date:** 08/15/03

Date: Thu, 14 Aug 2003 15:42:26 -0700

Dear Customer,

Thank you for contact Microsoft Online Support Service. My name is Pavan Pediredla and I will be working with you on this service request.

As I understand, you have 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."

If I have misunderstood, please feel free to let me know.

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:

[http://www.microsoft.com/security/security\\_bulletins/ms03-026.asp](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. You can find a link below to install the patch for Windows XP.

It is suggested that you first download the patch to your system so you can install the patch immediately after cleaning the system and before you reconnect to the Internet or network.

In some cases this Worm can cause your system to reboot and you may have difficulties downloading the patch. In those cases you need to turn off some ports that the virus uses by blocking them with Firewall software. The ports that may need to be blocked are as follows:

TCP/UDP Port 135

TCP/UDP Port 139

TCP/UDP Port 445

\*Note: Port 69 (TFTP) and TCP port 4444 are also in use by this worm and should be blocked.

The Internet Connection Firewall that comes with Windows XP will block these by default once it is enabled. To enable the Internet Connection Firewall that comes with XP do the following:

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.

To Download the patch and remove the Worm do the Following:

Step 1:

Download patch:

1. Download the patch for your system from the link shown below these steps.

<http://microsoft.com/downloads/details.aspx?FamilyId=2354406C-C5B6-44AC-9532-3DE40F69C074&displaylang>

Clean the worm from your system you should do one of the following:

2. Run your Antivirus software with an updated definitions.

and

Customers should use some of the online removal tools located at:

§

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

§ <http://vil.nai.com/vil/stinger>

§ <http://www.trendmicro.com/download/tsc.asp>

Install the patch:

3. Run the patch from the location you downloaded it to in step 1.

At the same time, we suggest you often go to <http://www.microsoft.com/security/> and install all critical updates and service packs from the Windows Update website: <http://windowsupdate.microsoft.com/>. In this way, your system is always protected from the potential security issues.

Once again I would like to thank you for contacting Microsoft Online Support Service. I am going to go ahead and close this case.

If you require further assistance with this issue, simply respond with any supplemental information. The case will then be reopened and forwarded back to me for follow-up.

If you have additional technical questions or concerns not related to this specific issue, please open up a new case. For your convenience I have included the following link:

<http://support.microsoft.com/support/webresponse.asp>

Again, thank you for choosing Microsoft.

Best Regards,

Pavan Pediredla

ARCR

=====  
A: Running Windows system connected to internet  
R: Computer shuts down unexpectedly  
C: DDOS attack which uses the bug of "Buffer Overrun in RPC Interface"  
R: Install 823980 patch  
=====

Adding updated disclaimer for posts made to newsgroups.

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

Please note I cannot respond to e-mailed questions.  
Please use these newsgroups to let me know if the suggestions resolved the issue.

"Steven Umbach" <n9rou@comcast.com> wrote in message  
news:nQF\_a.96573\$Vt6.31243@rwcrrnsc52.ops.asp.att.net...  
> *Did you go to <http://windowsupdate.com> ? Microsoft offers the patch*

to

> *remove the vulnerability. You need to go to a place like*  
> *<http://securityresponse.symantec.com/> for worm removal tools or update*

your

> *virus scanner to the latest definitions and try it. You also need to*  
install a

> *firewall to stay secure. -- Steve*

>

> *<http://www.microsoft.com/security/incident/blast.asp>*

> *<http://www.microsoft.com/security/articles/4steps.asp>*

>

> *"Maria" <jolu\_92@hotmail.com> wrote in message*

> *news:08d101c36225\$9e7d2720\$a501280a@phx.gbl...*

> > *I can't download the worm buster that microsoft is*

> > *offering. Any suggestions? Thank you!*

>

>