

Compass Rule Manger

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-05/1606.html

From: Cecil Dean (*anonymous_at_discussions.microsoft.com*)

Date: 05/10/04

Date: Sun, 9 May 2004 16:46:10 -0700

I got an e-mail from "Compass Rule Manger" with a fix for a problem I had. It reads as if it is third party working with Microsoft. The reply e-mail is compmail@microsoft.com.

Has anyone hear about this company and the repair fix they want me to do?

Thanks,
Cecil

This is a copy of the message,

Thank you for contacting Microsoft Support Services. We are contacting you because we understand; you may have received one of the following error messages when using your computer:

"LSA Shell (Export Version) encountered a problem and needed to close."

"lsass.exe - Application error. The instruction at "xxxxxxxxxxx" referenced memory at "xxxxxxxxxxx". The Memory could not be "read".

If your issue is not related to the errors above please contact Microsoft Support so we may assist you further.

The errors above are caused by a known Worm Virus issue. There is currently an Internet Worm Virus that is taking advantage of a security issue. Microsoft published a patch to fix the issue for all of the effected systems and to protect uninfected systems against attack on our web site. For more information, please refer to the following page:

<http://www.microsoft.com/technet/security/bulletin/ms04-011.msp>

The resolution to this issue is to install the patch and then clean the worm from your system. Please follow the instructions below in order to patch and clean an effected Windows 2000 or Windows XP operating system.

Instructions for patching and cleaning Windows 2000 and Windows XP systems.

1. To prevent LSASS.EXE from shutting down the machine during the cleaning process on Windows 2000 and Windows XP:

a. Unplug the network cable from the machine, or if the machine dials up to the Internet through a modem, do not establish a connection to the Internet yet (or if connected, disconnect).

i. This step is important as it will prevent a local copy of the worm from targeting the machine while performing the remaining steps.

2. This solution involves creating a read-only file named 'dcpromo.log' in the "%systemroot%\debug" directory and applies to both Windows 2000 and Windows XP operating systems. Creating this read-only file will prevent the vulnerability used by this worm from crashing the LSASS.EXE process on effected Windows operating systems by preventing the vulnerable code from being executed.

a. NOTE: %systemroot% is the variable that contains the name of the Windows installation directory. For example if Windows was installed to the "c:\winnt" directory the following command will create a file called dcpromo.log in the c:\winnt\debug directory.

The following commands must be typed in a command prompt (i.e. cmd.exe) exactly as they are written below.

i. To start a command shell, click Start and then click run and type 'cmd.exe' and press enter.

ii. Type the following command:
echo dcpromo >%systemroot%\debug\dcpromo.log

For this workaround to work properly you need to make the file read-only by typing the following command:

iii. attrib +R %systemroot%\debug\dcpromo.log

3. After creating the read-only dcpromo.log you can plug the network cable back in or dial out to the Internet and then download and install the MS04-011 patch from the MS04-011 download link before cleaning the system. If the system is cleaned before the patch is installed it is possible that the

system may be re-infected prior to installing the patch.

a. Here is the URL for the bulletin which contains the links to the download location for each patch:

<http://www.microsoft.com/technet/security/bulletin/ms04-011.msp>

b. If your machine is acting sluggish or that the Internet connection is slow you should use Task Manager to stop the following processes and then try downloading the patch again:

i. Stop any process ending with '_up.exe' (i.e. 12345_up.exe)

ii. Stop any process starting with 'avserv' (i.e. avserve.exe, avserve2.exe)

iii. Stop any process starting with 'skynetave' (i.e. skynetave.exe)

iv. Stop hkey.exe

v. Stop msiwin84.exe

vi. Stop wmiprvsw.exe

* Note there is a Windows system process called 'wmiprvse.exe' that should not be stopped.

c. Allow the system to reboot after the patch is installed.

4. Run the Sasser cleaner tool from the following URL:

a. For the on-line ActiveX control based version of the cleaner you can run it directly from the following URL:

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

b. For the stand-alone download version of the cleaner you can download it from the following URL:

<http://www.microsoft.com/downloads/details.aspx?>

FamilyId=76C6DE7E-1B6B-4FC3-90D4-9FA42D14CC17&displaylang=en

i. NOTE: If your machine is acting sluggish again or the Internet connection is slow, you should once again stop the processes outlined in step 3b above.

5. You should also determine if your machine may have been infected with a variant of the Agobot worm which also exploits the same security issue as the Sasser worm.
 - a. To do so run a full antivirus scan of their machine after ensuring your antivirus signatures are up to date.
 - b. If you do not have an antivirus product installed you can visit HouseCall from TrendMicro to perform a free scan using the following URL:
<http://housecall.trendmicro.com/>

6. Please visit the Protect Your PC web site for more