

Re: keep getting DCOM intrusions

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-11/1486.html>

From: David H. Lipman (*DLipman~nospam~_at_Verizon.Net*)

Date: 11/14/03

Date: Thu, 13 Nov 2003 19:43:59 -0500

The following was the response to the query "Is Win2003 uPnP compliant ?"....

"The UPnP(tm) feature set that is included in XP is not there. However, that does not mean that it won't support it in the future – it was in the earlier Betas and MS has been giving several demonstrations of UPnP technologies running on Server 2003, so is it "compliant" out of the box? The answer currently is no.

=D-

~ ~

Dave

"David H. Lipman" <DLipman~nospam~@Verizon.Net> wrote in message news:OWSzb3dqDHA.2692@TK2MSFTNGP09.phx.gbl...

| Bill:

|

| Of all people — I hate to disagree w/you but you are NOT correct and here is why....

|

| Let's first look at ICS, to use it we have to install ICS on a PC. That PC will need two NICs where one is connected to the ISP and the other is connected to a hub (or via a x-over

| cable to another PC). Right off the bat, the PC with ICS has one NIC directly exposed to the Internet and if that PC is a NT PC that has not been patched, it is exposed to RPCDcom exploitation. The PC has much overhead in that it has to have ICS loaded and has to provided services for two NICs. If the ISP is like Verizon DSL in former BellAtlantic territories than the PC with ICS will also need to have a PPPoE encapsulator. This could be

| RASPPPoE or WinPOET but that software will consume additional resources on the ICS PC. Plus

| that ICS PC will need its NIC connected to the WAN MTU set to 1492.

|

| With a Cable/DSL Router the LAN PCs are not exposed to the Internet as the Router sits between the WAN and the LAN. The Cable Router does not suffer from RPCDcom exploits. The LAN PCs are not encumbered in that no additional software is needed (ICS and PPPoE) and only

| one NIC is required in all LAN platforms. If the WAN connector is DSL that requires PPPoE then the Router will perform PPPoE and only the Router WAN port would need the MTU set to

microsoft.public.security.virus: Re: keep getting DCOM intrusions

| 1492. All the LAN platforms can remain at the standard MTU=1500.

|

| So the use of ICS and a Cable/DSL Router do not compare as they are completely different in

| that the use of a separate piece of equipment offloads the functionalities to that equipt.

| The Win32 platforms are not exposed to the Internet.

|

| As for uPnP, TCP port 5000, it is present on the LAN side of the Router not the WAN side of

| the Router. This will protect WinXP and WinME platforms from some form of uPnP attack.

| BTW: Is Win2003 Server also uPnP compliant