

Re: Port 135

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-10/1996.html>

From: Karl Levinson [x y] mvp (levinson_k_at_despammed.com)

Date: 10/17/03

Date: Fri, 17 Oct 2003 06:50:28 -0400

"Ed Martinez" <godbless@godbless.com> wrote in message
news:Ozc52sGIDHA.2216@TK2MSFTNGP12.phx.gbl...
> *Thank you, but that doesn't answer the question.*

I chose to only answer your second question.

Regarding your other question, I would want to go to a site such as
www.network-tools.com to look up the remote IP address or host name of the
computers connecting to your computer. This should give you an idea of
what's going on and why they're connecting to you. If you want to see if
you've been hacked, you could consider some of these steps:

<http://securityadmin.info/faq.htm#hacked>

<http://securityadmin.info/faq.htm#harden>

> *With the RPC/DCOM patches applies, with the Microsoft test utility
> indicating that the patch is applies, testing it locally and from remote,
> is there still something going on with this "hole" that leaves the port
> connected and established? In other words, did the patch do the job of
> stopping the vulnerability of this particular hole?*

The patch doesn't disable DCOM / RPC, so connections can still be made. And
even with a firewall, there could be connections from your machine to
itself, I suppose. That's why you need a firewall. If 135 is open [and
more importantly, all the other ports], there are other vulnerabilities that
can affect you, such as attackers being able to enumerate information.

If you're concerned about connections, the patch is not the thing to control
such a thing. A firewall is. In fact, if you were attacked with an RPC
buffer overflow, it's entirely possible that 135 would crash and could drop
all connections and stop listening, while you would likely have a shell
connection on another port entirely. That's the thing the patch is meant to
prevent, not connections.

> *There are times were I don't have the firewall up because it gets in the
way
> of testing. But in general, I have NO TCP/IP based services that are NOT*

That's not a great idea. Machines can be hacked in 15 minutes or less nowadays. As I said, there's usually a better way to get applications to work with the firewall still running. Also, if you really wanted complete control over your TCP/IP ports and services, you would use a firewall. Without a firewall, you often have no idea what applications and ports on your computer are really accessing the network.

> *under my control. Absolutely, no ports are being serviced who are not under*
> *my control. Unfortunately, we don't have control over PORT 135? Why is*
> *that Microsoft? If I turn off RPC, everything else "breaks" in Windows.*

What breaks exactly? It depends on your environment and what you want to do. Some people have done it. Or, alternatively you could consider disabling DCOM. If you want to use an application that depends on RPC, that's not really Microsoft's fault. Getting better security usually means disabling functionality, and the decision of how much security vs. functionality you want is entirely up to you.

Turning off services is only half the story and does NOT give you complete control over what your ports are doing, especially OUTBOUND. A firewall is still necessary to stop, say, a virus or trojan that gets on your machine via email or HTTP or what have you from opening up a new port or sending data outbound.

<http://securityadmin.info/faq.htm#closeports>

> *Sure, a firewall works, but a firewall is just a "KLUDGE" to the real*
> *PROBLEM.*

No. A firewall is not a kludge but an absolute necessity nowadays. There are ways to do packet filtering in the OS [using IPSec, for example], but these are IMHO totally insufficient, as there's no logging or alerting, for example. If you want better security features, you go to third party tools. That's always been true, whether you're running windows, linux, whatever. A large portion of *nix users run firewalls on the desktop, why shouldn't windows users do the same?

There are two real problems. 1) buffer overflows in DCOM / RPC. These are always going to exist and new ones are always going to come out requiring constant patches. However, there's also 2) it appears you want to run Windows networking and Windows management tools on your PC, only your OS has no adequate way of controlling which IP address has access to those services. No patch is going to fix that problem. It's commonly accepted security practice that if you want to use not terribly secure services like Windows networking and RPC and/or use more secure services to share sensitive data, that you use packet filtering to limit which networks and computers can access them... usually limited just to computers on your local network.

microsoft.public.security: Re: Port 135

Having said all that, whether or not to use a firewall is your choice. Some people do OK without them. But it's definitely a tool that gives you better security than not having one, and it's pretty much mandatory if you want to do what you're trying to do: have granular control over who connects to your TCP/IP ports and more knowledge about the purpose of each of those connections.

> *Why don't we have control over port 135? What is it about this service
> that this port must remain open?*

There are a number of articles at www.microsoft.com/technet/security and www.ntbugtraq.com [check the RPC / DCOM FAQ there] and www.google.com and www.google.com/advanced_group_search that explain what breaks when you disable RPC and/or DCOM over RPC.