

RE: WARNING! -- RPC ports on Win2k

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-11/0667.html>

From: LordInfidel (*LordInfidel_at_Directionweb.com*)

Date: 11/26/03

To: "'H. Nachtwandler'" <sleepwalker@saintly.com>, compjma@hotmail.com

Date: Wed, 26 Nov 2003 09:18:27 -0500

Just so everyone is clear on this,

If you are working in a domain or workgroup environment, want to share files between systems via

MS's sharing mechanism. Then you can not remove "client for ms networks" and "MS file and print sharing"

(Which effectively turns off RPC <135-139 and 445>).

However these ports should **NEVER** be allowed inbound or outbound through a firewall.

Next, I heard someone talk about IIS and its reliance on it, this is not true. However, if your

IIS server is multihomed with a front end interface (insecure internet facing, aka public) and a back end interface (pvt network to connect to other back end servers). Then you can not uninstall the 2 services, by doing so you remove them from all network adapters. Instead you simply unbind the services from the public interface (uncheck the pretty boxes).

On the flip side, if the server or workstation is a standalone host, that is it does not need to contact other MS machines for files or conduct domain level authentication. Then you can safely remove the 2 services bound from your network adapter and still operate without any repercussions on the local machine.

No machine on the public net, without a firewall in front of it to protect it, should have RPC ports listening, POINT BLANK!

LordInfidel

-----Original Message-----

From: H. Nachtwandler [mailto:sleepwalker@saintly.com]

Sent: Tuesday, November 25, 2003 12:16 PM

To: compjma@hotmail.com

Cc: security-basics@securityfocus.com

Subject: WARNING! -- RPC ports on Win2k

SecurityFocus BASICS: RE: WARNING! -- RPC ports on Win2k

Do not disable RPC service. Doing so will give you a bad afternoon, as I discovered the hard way.

Viz. --

[http://www.blackviper.com/WIN2K/win2kservice411.htm#Remote Procedure Call \(RPC\)](http://www.blackviper.com/WIN2K/win2kservice411.htm#Remote_Procedure_Call_(RPC))

> *Gift-shop online from the comfort of home at MSN Shopping! No crowds, free*

> *parking. <http://shopping.msn.com>*

>

>

>

>

>

----- Original Message -----

From: -----

Date: Tue, 25 Nov 2003 12:07:48 -0500

To: <sleepwalker@saintly.com>

Subject: FW: RPC ports on Win2k

>

>

> -----Original Message-----

> *From: Chris Berry [mailto:compjma@hotmail.com]*

> *Sent: Monday, 24 November 2003 17:52*

> *To: security-basics@securityfocus.com*

> *Subject: Re: RPC ports on Win2k*

>

>

> > *From: DIEGO PROTTA CASATI/6175/012/Graduacao <diego-casati@inatel.br>*

> > *I was wondering if anyone knows how to close the RPC ports on a Win2k*

> > *box.*

> > *Someone told me that it was possible. Anyone?*

>

> *Well, you could turn off the rpc service, enable tcp/ip filtering, and/or*

> *use a firewall.*

>

> *Chris Berry*

> *compjma@hotmail.com*

> *Systems Administrator*

> *JM Associates*

>

> *"The ability to destroy a planet is insignificant next to the power of the*

> *Force." --Darth Vader*

>

> _____

SecurityFocus BASICS: RE: WARNING! -- RPC ports on Win2k

--

Sign-up for Ads Free at Mail.com
<http://promo.mail.com/adsfreejump.htm>

