

Re: xp security vulnerabilities?

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-02/3688.html

From: cquirke (MVP Win9x) (*cquirkenews_at_nospam.mvps.org*)

Date: 02/23/04

Date: Mon, 23 Feb 2004 18:26:39 +0200

On Sat, 21 Feb 2004 11:15:04 -0000, "Robert Moir" <bofh@mvps.org>

>> *I have recently changed from Win98SE to WinXP corp pro, running Norton*

>> *Internet Security 2003. Under Win98 I had Atguard and BlackIce*

>> *running in addition to NIS and I came up undetected at every security*

>> *test site I could find.*

Be careful with running multiple apps that do the same things, as they can get in each other's way. Thinking multiple add-on firewalls, multiple "underfootware" antiviruses etc.

>> *I understand that WinXP has some (many?) holes and was wondering:*

>> *1. How important is it to install the SP's from MS, and what*

>> *"surprises" should I expect from them?*

>*Vital in my opinion.*

Some are definitely vital, with the RPC hole at the top of the list. I'd also apply SP1a (if it's not in place), the latest cumulative for IE 6 SP1, and the newly-released patch for ASN.1 hole.

I'd go further, though, and apply risk management over and beyond MS patches. MS patches block code flaws, but IMO as big a risk is posed by design flaws that MS thinks are a "good idea", such as hidden shares that provide access to the startup axis etc.

My general strategy:

- what you don't need, wall out
- what you may need, evaluate before risking
- what you risk, virus check first

This is at variance with MS's general approach of:

- make everything work
- spread a veneer of password/user security over the spiky bits
- assume that no-one out there will use these features for "evil"

>> 2. *What additional software should I have and/or what settings should I change in WinXP to be invisible on the net?*
>
> *"Invisible on the net" is a myth. You'll want to keep some kind of firewall running sure enough but you need to balance a need to get work done with a need to stay safe. A good firewall and virus scanner is a good start but there is no substitute for good common sense.*

Agreed; see the second step in the first list. Both you, and your PC, have to have "common sense"; watch out for scenarios where stupid software design says "yes" for you (IE's "Allow 3rd-party enhancements", "install on demand" etc.) or denies you the information you need to make an informed choice (e.g. "hide file name extensions")

>> 3. *Does Steve Gibson know what he's talking about or not?*

> *Ask 10 people that question and you might get 10 different answers. My opinion: He has one or two facts but he buries them in BS and hyperbole. His site is helpful to beginners perhaps but I don't know anyone in the security industry who takes him very seriously.*

He codes obsessively brilliantly, but his English programming is poor – full of big red exclamation marks etc. that make him look like an amateur. I think WAN networking is not his primary core competency (he's more of a disk dude) and that shows at times.

> *Ask yourself this question – Steve went on about how Raw Sockets in XP would cause the Internet to explode as soon as XP was released; How old is XP? And if you can read this reply, did the Internet blow up or not?*

Well, I'd not be **too** complacent about that, given we are still swamped with "why does my system keep restarting blah blah rpc blah blah nt authority lovesan nachi msblast yadda yadda" posts 6 months after the initial outbreak. While Win9x users just keep on truckin', wondering what all the "more secure" fuss is about.

Steve's problem was he got too specific – focussing purely on IP spoofing rather than taking a broader line on why XP was set to integrate so tightly with the mother of all infected networks.

RPC exists to allow arbitrary PCs to run processes on your PC, and it can't be turned off without the PC losing the ability to pick it's own nose. Does that sound like a smart design decision to you?

So of course when defects within this subsystem get whacked, you can't turn it off. You are supposed to download the fix via the same infected infosphere that is crashing your RPC service all the time, and because MS's duhfault setting is to "Restart the Computer" whenever the RPC service fails, the whole thing falls over every time.

microsoft.public.windowsxp.security_admin: Re: xp security vulnerabilities?

It's said that XP's built-in firewall blocks RPC attacks. Well, I dunno... I've just seen a PC that I set up to run this firewall, it's used by a newbie who doesn't fiddle (there are no forensic signs of fiddling either), the firewall's still set, and the PC was infected with variants B, E and F of Lovesan/Blaster. Hm.

>-- *Risk Management is the clue that asks:*

"Why do I keep open buckets of petrol next to all the ashtrays in the lounge, when I don't even have a car?"

>-----