

RE: [fw-wiz] terminal services

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-01/1572.html>

From: Paul D. Robertson (proberts@patriot.net)

Date: 01/28/03

From: "Paul D. Robertson" <proberts@patriot.net>

To: "Noonan, Wesley" <Wesley_Noonan@bmc.com>

Date: Tue Jan 28 17:39:16 2003

On Tue, 28 Jan 2003, Noonan, Wesley wrote:

> *I am not trying to pick on anyone here, but I have some
> comments/observations inline.*

Me too! Add me to the comment list!!!!1111 ;)

> *Through things like VPN connections in many cases. In others, you are*

Agreed, and hibernating laptops too– I think it should be a rule that some sort of extra laptop/VPN behaviour must happen on days like that.

> > *The issue isn't just that people inside
> > didn't patch their machines (though by my analysis, to a first
> > approximation virtually every machine they own was likely to be
> > vulnerable)*
>
> *I actually disagree here. The issue with slammer/sapphire is precisely that
> people didn't patch their machines. Let's review some of the recent history.*
>
> *1) Code Red. IIRC the patch against code red had been released almost 2
> months before Code Red hit, yet so many systems were still vulnerable.*

Worse (in terms of damage) was RDS, which was patched years before there was an exploit, but exploited more than anything else until we got the .printer stuff.

> *2) Nimda. Same thing. The patch against Nimda had been out for quite some
> time as well.*
> *3) Slammer/sapphire. The patch against slammer/sapphire was released in July
> of *last* year. We are talking about a patch that is well over 6 months old,
> IOW, a mature patch. That it was not applied in so many places is just
> embarrassing, especially after Code Red and Nimda.*

Yes, but if you look at all the patches and DLL versions, it's a twisty maze of patches, all seemingly alike.

Firewall-Wizards: RE: [fw-wiz] terminal services

For instance...

<http://ntbugtraq.ntadvice.com/default.asp?pid=36&sid=1&A2=ind0301&L=ntbugtraq&O=D&F=P&P=5163>

Is a post to NTBugtraq that details the versioning thing[1]. Clear as mud, and I'm not at all surprised that MS-based admins had trouble with untangling the patch issues surrounding this thing. Trust me, the primary data Russ used to get to that e-mail wasn't nearly as easy to figure out as it looks. ;)

Not only that, I think we can summarize by the 9AM Monday in Australia upshoot that MSDE was a bigger factor than SQL Server itself— and patching that wasn't a trivial task _if the user even *knew* it was necessary_— Now, I don't use MS Project, but if I did, I don't think I'd assume that SQL Server issues would affect my desktop.

Worse—yet, there are still third-party products where the vendor will *not support the product* if you apply the patch. Everything from CRM applications to door badge readers— there are raftloads of vendors of turnkey (or not) applications who aren't supporting customers who know they need to patch, let alone encouraging their customers to patch.

> > ; rather, it's that there was a hole. Mostly likely, there
> > was more than one hole, but it only took one, given how virulent this
> > worm was.
>
> No doubt, but the holes are secondary to what I believe the root problem is,
> which is laziness on the part of users, admins and vendors to apply patches
> in a timely fashion. I fully realize the costs of development, etc. but far
> too many people seem to think that once they install something, their
> responsibility is over. Patching systems is something that should be
> reviewed in the weekly security meetings and the patches should be applied
> on a regular and timely basis.

Didn't at least one of these patches have a memory leak associated with it?

> Now I also realize that people sometimes can't apply a patch because "vendor
> A says that their software hasn't been tested against that patch", but this
> is where the vendor culpabilities lie. Vendors need to stop sticking their
> heads in the sand or waiting for months to years for platform testing
> support (including spot checking for patches) which only leaves their
> customers vulnerable. It is irresponsible computing on so many levels that I
> think it takes away from the problem to simplify it as "don't open holes in
> your firewall".
>
> Anyway, enough from me. Again, not trying to pick on anyone here, but this
> has been a frequent conversation for me of late and I figured I would toss
> it out to the list as food for thought. Thanks.

Firewall-Wizards: RE: [fw-wiz] terminal services

While I'm sure there needs to be some sort of patching discipline, it's not a simple or clear-cut thing.

Paul

[1] Disclaimer, TruSecure owns NTBugtraq too, and there's an advertisement for something or other (for our people certification thing even) tacked on to the post. Might be advertising on the site too. It's probably a plot to lure you all into our wiley list trap...

Paul D. Robertson "My statements in this message are personal opinions proberts@patriot.net which may have no basis whatsoever in fact."
probertson@trusecure.com Director of Risk Assessment TruSecure Corporation