

RE: pcAnywhere...Outbound Only.

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-01/0585.html>

From: David Gillett (gillettdavid@fhda.edu)

Date: 01/30/03

From: "David Gillett" <gillettdavid@fhda.edu>

To: <security-basics@securityfocus.com>

Date: Thu, 30 Jan 2003 11:51:12 -0800

I had an interesting incident with this a few years back.

If you start up pcAnywhere as a client, without specifying a host, it will scan the Class C block you're on (*) for pcAnywhere-enabled hosts.

* – Unless they've since fixed it, it doesn't look at the net mask, it just blindly assumes that everyone is on a Class C subnet. Clueless.

Now what happened was that one of our employees was connected to our office VPN from home, and fired up pcAnywhere to talk to a server he was working on.

pcA took his home IP address, "deduced" the Class C block, and proceeded to port scan the block.

Now, because he was connected to our VPN, the scan requests travelled via the VPN to our office network, and tried to go out to the Internet via our NATting firewall....

So IF we had allowed outgoing pcA, potentially about 250 hosts, probably belonging to customers of the ISP he used, would have seen OUR OFFICE FIREWALL port-scanning them to see if they'd accept pcA connections. Any of them might have reported this to our ISP as an attack or hack attempt.

My recommendation is that if you allow pcA outbound, you allow it ONLY to specific hosts.

David Gillett

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

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

> Sent: January 28, 2003 13:33

> To: security-basics@securityfocus.com

> Subject: Re: pcAnywhere...Outbound Only.

>

RE: pcAnywhere...Outbound Only.

SecurityFocus BASICS: RE: pcAnywhere...Outbound Only.

>
> >From: "tony toni" <tony572001@hotmail.com>
> >We have a rule on our firewall that allows all employees to
> use pcAnywhere
> >to connect to a host OUTSIDE of our network. It is in one
> >direction...that is from inside our network to an outside
> host and not vise
> >versa. Our firewall administrator, came to me and asks me
> if I had any
> >security issues with this. He does not want the hassle of
> maintaining a
> >list of employees that can do this.
> >I do not see any glaring problems doing this....what do you think?
>
> As long as you are using a VPN this should be ok from a
> security point of
> view. If you're not using a VPN, try and get them to set
> both ends to at
> least symmetric encryption, preferably PKI, in the PC
> Anywhere settings.
> You wouldn't want those login passwords transmitted in the
> clear would you?
>
> >From a management point of view, just realize that people
> could use this to
> violate your company policies by taking control of their home
> computer and
> going to denied websites, playing video games, etc.
>
> Other than that, should be fine.
>
> Chris Berry
> compjma@hotmail.com
> Systems Administrator
> JM Associates
>
> "For Sys Admins paranoia isn't a mental health problem, its a
> marketable job
> skill."
>
>
>

> Tired of spam? Get advanced junk mail protection with MSN 8.
> <http://join.msn.com/?page=features/junkmail>
>