

Re: pcAnywhere Remote DoS

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2001-08/0023.html>

From: Steven Tracy (Steven@PRIMACOMPUTER.COM)

Date: 08/14/01

Message-ID: <5.0.0.25.0.20010814123149.034328e0@mail.primacomputer.com>
Date: Tue, 14 Aug 2001 12:49:52 +0800
From: Steven Tracy <Steven@PRIMACOMPUTER.COM>
Subject: Re: pcAnywhere Remote DoS
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

I run most of my web servers behind firewalls, or at least with most services unbound, so pcAnywhere is one of the few options I have to admin the machines short of going to site.

One way I have used to work around this, and other problems is with a small asp page that uses WSH to start/stop a service. Something like this:

```
<HTML>
<BODY>
Running Command<BR>
<%
    set wshell = server.createobject("wscript.shell")
    wshell.run "e:\le303mkjd9rnbs9\net start awhost32"
    set wshell = nothing
%>
Command Run<BR>
</BODY>
</HTML>
```

The "e:\le303mkjd9rnbs9\" is a directory outside the web root that contains a copy of net.exe, and any other things I need. Most executables under %SystemRoot% are Interactive:RX,Admin:F, and therefore can not be run by IUSR_xxxx, or System.

Best Regards,
Steven Tracy

At 09:21 PM 13-08-01, Sym Security wrote:
>Wed, 1 Aug 2001 14:17:35 -0400, John Thorton reported:
>
>Subject: pcAnywhere Remote DoS
>Comments: To: bugtraq@securityfocus.com
>Content-Type: text/plain; charset=iso-8859-1
>
>

