

# Re: EventID 529 Logged 1723 Times in one Day!

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-09/msg02711.html>

---

- From: David <David@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
  - Date: Wed, 19 Sep 2007 01:52:01 -0700
- 

Chris

Thanks for the prompt response.

I've closed all but ports 25, 123, 443, 444, 4125 and the uVNC ports. I've set the uVNC server service to manual and stopped it and had their ISP change the external IP address. So far so good.

--

David @ Solsletta

"Cris Hanna [SBS-MVP]" wrote:

Close Ports 80 and 21 immediately  
There is no reason for either to be open  
And change all passwords for all accounts immediately and start looking for other stuff

"David" <David@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:05DCF17C-B1BF-46C7-8488-C6CB96D60131@xxxxxxxxxxxxxxxxxxxx>  
Thanks for the prompt response. The usual ports are open for RWW, VPN & FTP plus VNC. So: 80, 25, 443, 444, 4125, 1723, 3389, 47, 123, 21 & VNC 5500,5800 & 5900. Std and I'm using a hardware firewall router with corresponding ports open. I guess I could change the port assignments.  
Any useful KB articles on same?

--

David @ Solsletta

"Cris Hanna [SBS-MVP]" wrote:

- > with all those different names, appears to be a hack attack
- > when you look at the event do you see an IP are they consistent?
- >

Re: EventID 529 Logged 1723 Times in one Day!

- > have you gone to www.grc.com and run Shields Up to see what's open?
- > Is port 80 open?
- > Is port 21 open for FTP?
- >
- > Are you running Std. or Premium?
- > If Std. what are you doing for a firewall?
- > "David" <David@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
- > [news:5B853CCB-3DB3-41A5-A7BB-7EA41680AB2B@xxxxxxxxxxxxxxxxxxxx](mailto:news:5B853CCB-3DB3-41A5-A7BB-7EA41680AB2B@xxxxxxxxxxxxxxxxxxxx)
- > This is appearing in the logswith varying User Names:
- >
- > Event Type: Failure Audit
- > Event Source: Security
- > Event Category: Logon/Logoff
- > Event ID: 529
- > Date: 14/09/2007
- > Time: 02:18:30
- > User: NT AUTHORITY\SYSTEM
- > Computer: MAC
- > Description:
- > Logon Failure:
- > Reason: Unknown user name or bad password
- > User Name: pop
- > Domain: MACPROSOL
- > Logon Type: 8
- > Logon Process: IIS
- > Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0
- > Workstation Name: MAC
- > Caller User Name: MAC\$
- > Caller Domain: MACPROSOL
- > Caller Logon ID: (0x0,0x3E7)
- > Caller Process ID: 2144
- > Transited Services: -
- > Source Network Address: -
- > Source Port: -
- >
- > The events are logged consistently but are intermittent. Generally
- > occurring every 2 seconds for several hours with one user name then
- > ceasing
- > for a few hours or days before starting with another user name.
- > Examples of
- > names are: pop, dns, test123, admin, administrator.
- >
- > Hack attempt and apart from turning off remote access any ideas?
- > --
- > David @ Solsletta
- >