

Re: Security error, EventID 529

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-03/msg00570.html>

- *From:* "jason" <jasonsantos-NOSPAM-@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 3 Mar 2006 09:06:51 -0500
-

Thanks for the reply, Brandy.

It seems where this is happening is actually on my server, and the process ID is related to Store.exe or Exchange. Like I mentioned before, the username it refers to is mine, but I never use it to log into the server locally, only on my workstation. Any further help would be appreciated.

Jason

""Brandy Nee [MSFT]"" <v-branee@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:MO0IKZoPGHA.5536@xxxxxxxxxxxxxxxxxxxxxxxx

Hello Jason,

Thank you for posting to the SBS Newsgroup.

I understand that you got many Event ID 529 on your SBS 2K3 Server. If I have misunderstood your concern, please let me know.

Based on my experience, this kind of issue may be caused by Application logon such as while Outlook is connecting to Exchange Server, or this is an automated dictionary attack on weak passwords. The hacker is trying variable username/password (here it is webmaster) combinations to access the network. The attack can be initiated from internal network or external network.

In the event log you included, I noticed that the logon type is 3, which means Network logon. The "Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0" is the default authentication package; Advapi means "API call to LogonUser". Based on these event attributes, it is most likely that the hacker is attempting to logon the Exchange services such as OWA or SMTP.

You can check to see which process handles the session. For example, in this event, the Caller Process ID is 6936. Write down the process ID, go to

Re: Security error, EventID 529

problematic computer where user account jsantos is logon from, press Ctrl+Alt+Del and click "Task Manager". In the task manager window, click "Processes" tab. Click "View"--->"Select Columns". Check "PID (Process Identifier)" and click "OK". In the process list, find the process with 6936 PID. What's the process?

I also suggest that you perform a clean boot on the problematic computer:

- a. Click Start-->Run, type "MSCONFIG" (without the quotation marks) and click OK.
- b. In the System Configuration Utility (MSConfig) window, click the "Startup" tab.
- c. Click to clear all the check marks from the list box under "Startup".
- d. Click the Services tab, check the "Hide all Microsoft Services" box and then click the "Disable All" button to disable the non-Microsoft services.
- e. Click OK to close the MSConfig window. Click Yes when you are asked to restart your computer in order to enable the changes.
- f. After restarting, please check whether this issue still exists.

Technically speaking, we cannot prevent a hacker attacking your server. We can ignore the events as the attack was unsuccessful. However, since it indicates the hacker attacking, I strongly suggest that we perform following steps to improve the network security:

1. Scan virus on the computers. Please use the anti-virus software to perform full scan on the internal computers. There is an online virus scan link below:

<http://housecall.trendmicro.com/>

2. Implement Strong password policies. Open "Server Management console", navigate to Users snap-in. In the right panel, click "Configure Password Policies". Enable the password policies. You'd better also ask your users to change their passwords to avoid successfully attack against weak password.

For more information:

Account Passwords and Policies

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/bpactlck.mspx>

3. Monitor the internal users to see if anyone is testing the admin accounts.
4. Please have a look at following White Paper to secure your SBS Network.

Re: Security error, EventID 529

Securing Your Windows Small Business Server 2003 Network

<http://www.microsoft.com/downloads/details.aspx?FamilyID=f62b2722-267c-4642-b287-c31115ef10a4&DisplayLang=en>

Please take your time to read through my suggestions and perform the steps.

If you have any updates, please feel free to let me know. I am looking forward to hearing from you!

Best regards,

Brandy Nee

Microsoft CSS Online Newsgroup Support

Get Secure! – www.microsoft.com/security

=====

This newsgroup only focuses on SBS technical issues. If you have issues regarding other Microsoft products, you'd better post in the corresponding newsgroups so that they can be resolved in an efficient and timely manner.

You can locate the newsgroup here:

<http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>

When opening a new thread via the web interface, we recommend you check the

"Notify me of replies" box to receive e-mail notifications when there are any updates in your thread. When responding to posts via your newsreader, please "Reply to Group" so that others may learn and benefit from your issue.

Microsoft engineers can only focus on one issue per thread. Although we provide other information for your reference, we recommend you post different incidents in different threads to keep the thread clean. In doing so, it will ensure your issues are resolved in a timely manner.

For urgent issues, you may want to contact Microsoft CSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

Any input or comments in this thread are highly appreciated.

=====

This posting is provided "AS IS" with no warranties, and confers no rights.

From: "jason" <jasonsantos-NOSPAM-@xxxxxxxxxxxxxxxxxxxxxxxx>
Subject: Security error, EventID 529

Re: Security error, EventID 529

Date: Thu, 2 Mar 2006 13:53:27 -0500
Lines: 30
X-Priority: 3
X-MSMail-Priority: Normal
X-Newsreader: Microsoft Outlook Express 6.00.2900.2180
X-RFC2646: Format=Flowed; Original
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
Message-ID: <#CdjYqiPGHA.456@xxxxxxxxxxxxxxxxxxxxxxxx>
Newsgroups: microsoft.public.windows.server.sbs
NNTP-Posting-Host: pool-71-99-239-121.tampfl.dsl-w.verizon.net

71.99.239.121

Path:
TK2MSFTNGXA03.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP15.phx.gbl
Xref: TK2MSFTNGXA03.phx.gbl
microsoft.public.windows.server.sbs:248832
X-Tomcat-NG: microsoft.public.windows.server.sbs

Using SBS2003 SP1 and XP Pro.

I've been getting over 100 errors a day regarding an EventID 529:

Logon Failure:
Reason: Unknown user name or bad password
User Name: jsantos
Domain:
Logon Type: 3
Logon Process: Advapi
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: SBSSERVER
Caller User Name: SBSSERVER\$\br/>Caller Domain: WORKPLACE
Caller Logon ID: (0x0,0x3E7)
Caller Process ID: 6936
Transited Services: -
Source Network Address: -
Source Port: -

I can't figure out how to stop this. The username it's referring to is
mine,

but I can login to any workstation just fine.

Any ideas?

Thanks.
Jason

Re: Security error, EventID 529