

# Re: Weird 529 Errors in Security Log

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-04/msg00016.html>

---

- *From:* "Bill Glidden" <billyg1943@xxxxxxxxxxxx>
  - *Date:* Sun, 1 Apr 2007 10:49:14 +1000
- 

OK, after implementing strong passwords, I got 6,992 of these errors in the last 24 hours! Are you sure someone is not attempting an intrusion? Bit scary.

"Les Connor [SBS MVP]" <les.connor@xxxxxxxxxxxx> wrote in message <news:427ACD11-EC5B-428B-9D18-331285026017@xxxxxxxxxxxxxxxxxxxx>

Bill,

Those attempts are, ahem, normal. They come in waves, and seem to circulate IP ranges. I've got a number of SBS boxes on 3 different ISP's. One night, all the servers on ISP A get a wave of these. Then a few days later, ISP B, then C.

I haven't seen any in a while (few weeks), so they're presumably working on an IP range far from me, and quite close to you ;-).

There isn't much you can do about it, unless you want to go blocking whole ranges of IP's that represent the originating geographic locations.

If your passwords are secure, you should be OK.

--

Les Connor [SBS MVP]

"Bill Glidden" <billyg1943@xxxxxxxxxxxx> wrote in message <news:O189T5ycHHA.4888@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Hi Terence,

There were sixty-one 529 events in the last 24 hours all similar to the following:

    Usernames such as: root, www, server, admin, administrator, web, webmaster, data, etc.

    Logon type: 3

    Logon process: Advapi

Re: Weird 529 Errors in Security Log

Authentication Package:  
MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Workstation name: sbsserver  
Callers User Name: sbsserver\$\br/>Caller domain: domain  
Caller logon ID: (0x0,0x3E7)  
Caller process ID: 1140  
Transited Services: –  
Source Network Address: –  
Source Port: –

Is this a hacking attempt?

I have enabled strong password policy.

Sorry if the scope has changed – do you want me to start a new thread?

Cheers,  
Bill

"Terence Liu [MSFT]" <v-terliu@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
message  
[news:Qe7UITqcHHA.6068@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:Qe7UITqcHHA.6068@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hello Bill,

Thank you for kind update.

Base on my knowledge, 8 event logs of 529 per day is normal for SBS. For example: if one user enter wrong password when logon domain, the SBS will log event 529 one time. However, if you still want to narrow down the error, we can go through the following steps:

Do all event errors Source Network Address are one workstation? If yes, please pay more attention on this workstation:

1. Do clean boot on this problematic workstation:
  - a. Click Start, click Run, and then in the Open box, type "MSCONFIG" (without the quotation marks). Click OK.
  - b. In the System Configuration Utility (MSConfig) window, click to select the Selective Startup button.

## Re: Weird 529 Errors in Security Log

- c. Click to clear the check mark from the "Load startup items" below Selective Startup.
  - d. Click the Services tab, click to check the "Hide All Microsoft Services" box, and remove all the check marks from the remained Non-Microsoft Services. Please note that the Exchange services could be marked as non-Microsoft. Please do not disable those 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 will reoccur.
2. There are some viruses will try to attack domain controller, please install latest antivirus software on the problematic workstation and then do full scan on it.
  3. Monitor the internal users to see if anyone is testing the admin accounts.

If not from one workstation, please perform the following steps:

1. Implement Strong password policies on SBS. Open "Server Management console", navigate to Users snap-in. In the right panel, click "Configure Password Policies". Enable the password policies.

For more information:

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

2. Check in Scheduled Tasks and see if there are any tasks running as the administrator account, if there are, make sure the password is configured

Re: Weird 529 Errors in Security Log

properly.

Hope these steps will give you some help.

Thanks and have a nice day!

Best regards,

Terence Liu(MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – [www.microsoft.com/security](http://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

Re: Weird 529 Errors in Security Log

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: "Bill Glidden" <billyg1943@xxxxxxxxxxxx>  
| References:  
| <#fZ4OambHHA.1240@xxxxxxxxxxxxxxxxxxxxxx>  
| <Nte6Jt2bHHA.928@xxxxxxxxxxxxxxxxxxxxxx>  
| <ejBxD#YcHHA.3632@xxxxxxxxxxxxxxxxxxxxxx>  
| <oINQiXdcHHA.3744@xxxxxxxxxxxxxxxxxxxxxx>  
| Subject: Re: Weird 529 Errors in Security Log  
| Date: Fri, 30 Mar 2007 09:02:13 +1000  
| Lines: 349  
| X-Priority: 3  
| X-MSMail-Priority: Normal  
| X-Newsreader: Microsoft Outlook Express 6.00.2900.3028  
| X-MimeOLE: Produced By Microsoft MimeOLE  
| V6.00.2900.3028  
| X-RFC2646: Format=Flowed; Original  
| Message-ID:  
| <eCcsNZlcHHA.4888@xxxxxxxxxxxxxxxxxxxxxx>  
| Newsgroups: microsoft.public.windows.server.sbs  
| NNTP-Posting-Host: 203-206-187-213.perm.iinet.net.au  
| 203.206.187.213  
| Path:  
| TK2MSFTNGHUB02.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP02.phx.gbl  
| Xref: TK2MSFTNGHUB02.phx.gbl  
| microsoft.public.windows.server.sbs:26524  
| X-Tomcat-NG: microsoft.public.windows.server.sbs  
|  
| Hi Terence,  
|  
| Only had eight 529 error in this morning's Security Log all  
| similar to  
| this:  
|  
| Event Type: Failure Audit  
| Event Source: Security  
| Event Category: Logon/Logoff  
| Event ID: 529  
| Date: 30/03/2007  
| Time: 8:06:21 AM  
| User: NT AUTHORITY\SYSTEM  
| Computer: <SBS Server>  
| Description:

Re: Weird 529 Errors in Security Log

| Logon Failure:  
| Reason: Unknown user name or bad password  
| User Name: anonymous  
| Domain:  
| Logon Type: 3  
| Logon Process: Advapi  
| Authentication Package:  
MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
| Workstation Name: <SBS Server>  
| Caller User Name: <SBS Server>  
| Caller Domain: <My Domain>  
| Caller Logon ID: (0x0,0x3E7)  
| Caller Process ID: 1140  
| Transited Services: –  
| Source Network Address: –  
| Source Port: –

| For more information, see Help and Support Center at  
<http://go.microsoft.com/fwlink/events.asp>.

| This is an improvement on the 50–100 errors before I ran  
NETDOM  
RESETPWD.

| The errors now seem to be different and there is more  
information in  
the  
log. Should I continue with your suggestions or is there  
something  
else  
you  
could suggest?

| Cheers,  
| Bill Glidden

| "Terence Liu [MSFT]"  
<v-terliu@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
| [news:oINQiXdcHHA.3744@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:oINQiXdcHHA.3744@xxxxxxxxxxxxxxxxxxxxxxxx)

| > Hello Bill,  
| >  
| > Thank you for your kind update.  
| >  
| > I was just writing to say that I hope everything is going  
well.  
| >  
| > Please do not hesitate to let me know if this problem  
reoccurs or if  
| > there's anything else I can do for you.  
| >  
| > Thank you and have a nice day,

Re: Weird 529 Errors in Security Log

|>  
|> Best regards,  
|>  
|> Terence Liu(MSFT)  
|>  
|> Microsoft CSS Online Newsgroup Support  
|>  
|> Get Secure! – [www.microsoft.com/security](http://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.

Re: Weird 529 Errors in Security Log

|>  
|> 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: "Bill Glidden" <billyg1943@xxxxxxxxxxxx>

|> | References:

<#fZ4OambHHA.1240@xxxxxxxxxxxxxxxxxxxx>

|> | <Nte6Jt2bHHA.928@xxxxxxxxxxxxxxxxxxxx>

|> | Subject: Re: Weird 529 Errors in Security Log

|> | Date: Thu, 29 Mar 2007 09:19:14 +1000

|> | Lines: 199

|> | X-Priority: 3

|> | X-MSMail-Priority: Normal

|> | X-Newsreader: Microsoft Outlook Express

6.00.2900.3028

|> | X-MimeOLE: Produced By Microsoft MimeOLE

V6.00.2900.3028

|> | X-RFC2646: Format=Flowed; Original

|> | Message-ID:

<ejBxD#YcHHA.3632@xxxxxxxxxxxxxxxxxxxx>

|> | Newsgroups: microsoft.public.windows.server.sbs

|> | NNTP-Posting-Host:

203-206-187-213.perm.iinet.net.au

203.206.187.213

|> | Path:

TK2MSFTNGHUB02.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP02.phx.gbl

|> | Xref: TK2MSFTNGHUB02.phx.gbl

microsoft.public.windows.server.sbs:26228

|> | X-Tomcat-NG: microsoft.public.windows.server.sbs

|> |

|> | Hi Terence,

|> |

|> | Thank you for responding.

|> |

|> | All my XP Pro PCs are already at SP2. My SBS 2003  
server is at SP1

and I

Re: Weird 529 Errors in Security Log

|> am  
|> | not going to go to SP2 until well known issues are resolved!  
|> |  
|> | I have just applied NETDOM RESETPWD and will reboot soon. I will check  
|> the  
|> | event log tomorrow and see whether this was the issue. If not, I will  
|> press  
|> | on with your other suggestions.  
|> |  
|> | Cheers,  
|> | Bill Glidden  
|> |  
|> | "Terence Liu [MSFT]"  
<v-terliu@xxxxxxxxxxxxxxxxxxxxxx> wrote in message  
|> |  
[news:Nte6Jt2bHHA.928@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:Nte6Jt2bHHA.928@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)  
|> |> Hello Bill,  
|> |>  
|> |> Thank you for posting here.  
|> |>  
|> |> According to your description, I understand that you get many event  
|> logs  
|> |> 529 from one workstation. If I have misunderstood the problem, please  
|> |> don't  
|> |> hesitate to let me know.  
|> |>  
|> |> Based on my research, I suggest we try the following steps to see  
if  
|> we  
|> |> can  
|> |> resolve this issue:  
|> |>  
|> |> 1: Install latest service pack for workstation and SBS server:  
|> |>  
|> |> How to obtain the latest Windows XP service pack  
|> |> <http://support.microsoft.com/?id=322389>  
|> |>  
|> |> How to obtain the latest service pack for Windows

Re: Weird 529 Errors in Security Log

Server 2003

|> |> <http://support.microsoft.com/?id=889100>

|> |>

|> |> 2. There are several running processes on the SBS server that

will

|> attempt

|> |> to connect using the machine account.

|> |> One of the most active is the Microsoft Exchange Routing Engine.

|> |>

|> |> This behavior can happen when the machine password is not

properly

|> sync.

|> |>

|> |> In order to reset the machine account password of a domain

controller

|> use:

|> |>

|> |> NETDOM RESETPWD /Server:ServerName  
/UsedD:Administrator  
/PasswordD:\*

|> |>

|> |> The syntax of this command is:

|> |> NETDOM RESETPWD /Server:domain-controller  
/UserD:user

|> /PasswordD:[password

|> |> |\*]

|> |>

|> |> NETDOM RESETPWD Resets the machine account password for the

domain

|> |> controller

|> |> on which this command is run. Currently there is no support for

|> resetting

|> |> the machine password of a remote machine or a member server. All

|> |> parameters

|> |> must be specified.

|> |>

|> |> /Server Name of a specific domain controller that should

have

|> its

|> |> machine account password reset.

|> |>

|> |> /UserD User account used to make the connection with the

## Re: Weird 529 Errors in Security Log

|> domain  
|> |> controller specified by the /Server argument.  
|> |>  
|> |> /PasswordD Password of the user account specified  
with  
/UserD.  
A  
|> \*  
|> |> means  
|> |> to prompt for the password  
|> |>  
|> |> After completing the command, reboot the server.  
|> |>  
|> |> 3. As I know, some 3rd-party software will refer to  
this issue  
if  
they  
|> |> trying to use invalid credentials to log on to IIS. I  
suggest we  
try  
|> to  
|> do  
|> |> clean boot to narrow down it:  
|> |>  
|> |> To clean boot the server, please use the steps below:  
|> |> a. Click Start, click Run, and then in the Open box,  
type  
"MSCONFIG"  
|> |> (without the quotation marks). Click OK.  
|> |>  
|> |> b. In the System Configuration Utility (MSConfig)  
window, click  
to  
|> select  
|> |> the Selective Startup button.  
|> |>  
|> |> c. Click to clear the check mark from the "Load startup  
items"  
below  
|> |> Selective Startup.  
|> |>  
|> |> d. Click the Services tab, click to check the "Hide All  
Microsoft  
|> |> Services"  
|> |> box, and remove all the check marks from the  
remained  
Non-Microsoft  
|> |> Services. Please note that the Exchange services could  
be marked  
as  
|> |> non-Microsoft. Please do not disable those services.

Re: Weird 529 Errors in Security Log

|> |>  
|> |> 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 will reoccur.  
|> |>  
|> |> 4. Scan virus on the SBS and all workstations. Please use the  
|> anti-virus  
|> |> software to perform full scan on the internal network. There is  
an  
|> online  
|> |> virus scan link below:  
|> |>  
|> |> <<http://housecall.trendmicro.com/>>  
|> |>  
|> |> 5. 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.  
|> |>  
|> |> For more information:  
|> |>  
|>  
<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies>  
|> |> /security/bpactlck.mspx>  
|> |>  
|> |> 6. Monitor the internal users to see if anyone is testing the  
admin  
|> |> accounts.  
|> |>  
|> |> 7. Check in Scheduled Tasks and see if there are any tasks  
running  
as  
|> the  
|> |> administrator account, if there are, make sure the password is  
|> configured  
|> |> properly.  
|> |>  
|> |> If the issue persists, please kindly help me collect

Re: Weird 529 Errors in Security Log

some  
information  
> for  
> > further investigation:  
> >  
> > Save the application event log and system event log as  
evt files  
on  
> the  
> > problematic machines and send to my mailbox:  
v-terliu@xxxxxxxxxxxxxx  
> >  
> > Hope these steps will give you some help.  
> >  
> > Thanks and have a nice day!  
> >  
> > Best regards,  
> >  
> > Terence Liu(MSFT)  
> >  
> > 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

Re: Weird 529 Errors in Security Log

|> 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: "Bill Glidden" <billyg1943@xxxxxxxxxxxx>  
|> |> | Subject: Weird 529 Errors in Security Log  
|> |> | Date: Sun, 25 Mar 2007 08:48:33 +1000  
|> |> | Lines: 15  
|> |> | X-Priority: 3  
|> |> | X-MSMail-Priority: Normal  
|> |> | X-Newsreader: Microsoft Outlook Express  
6.00.2900.3028  
|> |> | X-MimeOLE: Produced By Microsoft MimeOLE  
V6.00.2900.3028

Re: Weird 529 Errors in Security Log

|> |> | X-RFC2646: Format=Flowed; Original  
|> |> | Message-ID:  
<#fZ4OambHHA.1240@xxxxxxxxxxxxxxxxxxxxxx>  
|> |> | Newsgroups: microsoft.public.windows.server.sbs  
|> |> | NNTP-Posting-Host:  
203-206-187-213.perm.iinet.net.au  
203.206.187.213  
|> |> | Path:  
|>  
TK2MSFTNGHUB02.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP04.phx.gbl  
|> |> | Xref: TK2MSFTNGHUB02.phx.gbl  
|> |> | microsoft.public.windows.server.sbs:25269  
|> |> | X-Tomcat-NG: microsoft.public.windows.server.sbs  
|> |> |  
|> |> | Started getting many of these in event log. All from  
one  
|> |> | workstation,  
|> |> | sometimes over 50 a day. Any ideas, anyone?  
|> |> |  
|> |> | Reason: Unknown user name or bad password  
|> |> | User Name: <name>@hotmail.com  
|> |> | Domain:  
|> |> | Logon Type: 3  
|> |> | Logon Process: NtLmSsp  
|> |> | Authentication Package: NTLM  
|> |> | Workstation Name: <fred>  
|> |> |  
|> |> | TIA,  
|> |> | Bill  
>	>
>	>
>	>
>	>
>	>
>	
>	
>	
>	