

# Re: Login Error – Microsoft authentication package v1

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-01/msg03693.html>

---

- *From:* "Teneo" <not@xxxxxxx>
  - *Date:* Tue, 29 Jan 2008 14:59:23 -0000
- 

Hi Manfred, thanks for the information always a great help.

The process is inetinfo, and my conclusion ( my post was to help others) was it was an attempt on port 25 SMTP..

We are reviewing OWA / RWW failed logins but we cant seem to find where to turn logging on as any failed attempts dont seem to generate any alerts... Any pointers would be great..

"Manfred Zhuang [MSFT]" <v-mzhuan@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:1OFwjImYIHA.360@xxxxxxxxxxxxxxxxxxxxxxxx>

Hello Teneo,

Thank you for posting here.

From your post, I understand that some security warnings are found in event log.

This is probably an automated dictionary attack on weak passwords. The hacker is trying variable username/password combinations to access the network. The attack can be initiated from internal network or external network. According to the message, Logon type 3 means Network logon; Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0 is the default authentication package; advapi means "API call to LogonUser". 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 process ID is 1716. Write down the process ID, Ctrl+Alt+Del and click Task Manager. On the Processes tab. Click View -> Select Columns. Check PID (Process Identifier) and click OK. In the process list, find the

Re: Login Error – Microsoft authentication package v1

process with the PID of 1716. What's the process?

Since it indicated the hacker attacking, I'd like to give the following suggestions to improve the network security:

1. Scan virus on the workstations and the servers. Make sure the virus software is up to date.
2. Implement Strong password policies. Click Start, click Server Management and click Users. In the right pane, click Configure Password Policies and configure the password policies.

Account Passwords and Policies

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

3. Disable the Guest account.
4. Refer to the following document for more details:

Securing Your Windows Small Business Server 2003 Network

[http://www.microsoft.com/technet/security/secnews/articles/sec\\_sbs2003\\_network.mspx](http://www.microsoft.com/technet/security/secnews/articles/sec_sbs2003_network.mspx)

Hope this helps.

Please feel free to let me know if you have any questions or if you need further assistance.

I'm looking forward to hearing from you.

Best regards,

Manfred Zhuang(MSFT)  
Microsoft 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

Re: Login Error – Microsoft authentication package v1

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: "Teneo" <not@xxxxxxx>  
| Subject: Login Error – Microsoft authentication package v1  
| Date: Mon, 28 Jan 2008 07:42:49 –0000  
| Lines: 72  
| X-Priority: 3  
| X-MSMail-Priority: Normal  
| X-Newsreader: Microsoft Outlook Express 6.00.2900.3138  
| x-mimeole: Produced By Microsoft MimeOLE V6.00.2900.3198  
| X-RFC2646: Format=Flowed; Original  
| Message-ID: <ubPVjFYIHA.4476@xxxxxxxxxxxxxxxxxxxxxx>  
| Newsgroups: microsoft.public.windows.server.sbs  
| NNTP-Posting-Host: mail.sxcomputers.co.uk 217.37.113.169  
| Path: TK2MSFTNGHUB02.phx.gbl!TK2MSFTNGP01.phx.gbl!TK2MSFTNGP06.phx.gbl  
| Xref: TK2MSFTNGHUB02.phx.gbl microsoft.public.windows.server.sbs:89031  
| X-Tomcat-NG: microsoft.public.windows.server.sbs  
|  
| Logon Failure:  
|  
| Reason:  
| Unknown user name or bad password  
|  
| User Name:  
| 12345  
|  
| Domain:  
|  
| Logon Type:  
| 3  
|

Re: Login Error – Microsoft authentication package v1

|  
| Logon Process:  
| Advapi  
|  
| Authentication Package:  
| MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
|  
| Workstation Name:  
| SERVER  
|  
| Caller User Name:  
| SERVER\$  
|  
| Caller Domain:  
| own domain name here, changed by me.  
|  
| Caller Logon ID:  
| (0x0,0x3E7)  
|  
| Caller Process ID:  
| 1716  
|  
| Transited Services:  
| –  
|  
| Source Network Address:  
| –  
|  
| Source Port:  
| –  
|  
| Seen this posted before but couldn't find orig details and maybe its way  
| back down the list so thought post again.  
|  
| I have found that this is related to login on port 25. (SMTP) if not  
| aware  
| that password on port 25 is base64. Testing with normal password  
| gives gobbledook. Try login with base64 username and password and get  
| exact  
| result.

Re: Login Error – Microsoft authentication package v1

|  
| Seeing alot of attacks on port 25 recently.  
|  
|  
|