

Secure Channel problem

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-02/0023.html>

From: Carnegie, Martin (*Martin.Carnegie_at_ATCOITEK.COM*)

Date: 02/13/04

Date: Fri, 13 Feb 2004 14:08:05 -0700
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Hi All,

Hopefully you don't mind this question to the list, but we have been working on a problem for the past year with no solution.

Environment:

Single Win2k SP3 and 4 domain
Approx 140 Win2k member servers
Approx 4000 WinXP workstations

Here is the problem.

On random servers we are seeing a domain group that is added to a local group using the GPO. When the GPO runs we will see the following 2 messages in the Application log

Source: Userenv
Event ID: 1000
User: AUTHORITY\SYSTEM
The Group Policy client-side extension Security was passed flags (17) and returned a failure status code of (5).
For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Source: SceCli
Event ID: 1202
User: N/A
Security policies are propagated with warning. 0x5 : Access is denied.
Please look for more details in Troubleshooting section in Security Help.
For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Then in the winlogon.log
----Configure Group Membership...
 Configure Tivoli_Admin_Privileges.
Match - <renamed ADMINISTRATOR USERID>.

NT-Bugtraq: Secure Channel problem

Match – SYSTEM.

add *S-1-5-21-174793946-378299862-635260049-53312.

Error 1387: A member could not be added to or removed from the local group because the member does not exist.

error adding

*S-1-5-21-174793946-378299862-635260049-53312.

Match – SID: S-1-5-21-1390067357-616249376-682003330-500.

Match – SID: S-1-5-18.

Configure Power Users.

Match – <local USERID>.

Match – SID: S-1-5-21-1390067357-616249376-682003330-1003.

Once this happens we are unable to use our systems management product (Tivoli) to do anything on the server. The only fix is to use the netdom reset command or to reboot the computer. Either way will reset the secure channel.

We were hoping that SP4 would have addressed this issue, but I have seen the problem on a SP4 server now.

Here is a link that contains some more information

<http://support.microsoft.com/default.aspx?scid=kb:en-us:306100&Product=win2000>

We are also seeing this message in the system log on the domain controllers

Source: NETLOGON

User: N/A

Event ID: 5722

The session setup from the computer <servername> failed to authenticate.

The name of the account referenced in the security database is

<servername>\$. The following error occurred:

Access is denied.

Here is an article on this:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:288167>

Thanks for any information.

Martin Carnegie

ATCO I-Tek

Phone: 780.420.5068

Pager: 780.671.2895

mailto:martin.carnegie@atcoitek.com

The information transmitted is intended only for the addressee and may contain confidential, proprietary and/or privileged material. Any unauthorized review, distribution or other use of or the taking of any

NT-Bugtraq: Secure Channel problem

action in reliance upon this information is prohibited. If you receive this in error, please contact the sender and delete or destroy this message and any copies.

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which automatically notifies the perceived sender of a message it believes is infected may well cause more harm than good. Someone who did not actually send you a virus may receive the notification and scramble their support staff to find an infection which never existed in the first place. Suggest such notifications be disabled by whomever is responsible for your AV, or at least that the idea is considered.
