

Re: Computer Management Security Problem

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-07/1305.html>

From: Mark-Allen (*mark-allen_at_mvps_dot_org*)

Date: 07/29/04

Date: Thu, 29 Jul 2004 01:07:23 +0200

I agree with Paul. Sounds like an inadvertent group addition.

Check: To view a user's group membership for a domain(s), use the resource kit utility Showgrps.exe..

Run it under the user account that appears to have too many privileges.

--

Mark-Allen Perry

ALPHA Systems, Switzerland

mark-allen AT mvps DOT org

"Paul Adare - MVP - Microsoft Virtual PC" <padare@newsguy.com> wrote in message news:MPG.1b713b

In article <FBA54439-EE5A-4BA4-8758-663657A38370@microsoft.com>, in the

microsoft.public.win2000.security news group, =?Utf-8?B?RGF2ZSBXLg==?=

<DaveW@discussions.microsoft.com> says...

> All users are part of the "Domain Users" group which belongs to the "Administrators" group in
>

So, you're using Restricted Groups in Group Policy to add the Domain Users group to the Administrators group? And I'm betting that you're either using the Default Domain GPO or a GPO at the domain level to enforce this? This is your problem right here.

By using a GPO at the domain level and specifying that Domain Users are members of a group called Administrators, not only are you adding Domain Users to the local Administrators group on your workstations, you're also adding Domain Users to the Administrators group on your Domain Controllers!!!

There are a number of ways to fix this:

1. Make sure that all affected workstations are in an OU (not the default Computers container as that is not an OU) and then create a GPO with your restricted groups setting that only applies to the workstations.

2. If you insist on using a domain level GPO for this, modify the Default Domain Controllers GPO to not include Domain Users in the Administrators group.

You've done this to yourself and has nothing specifically to do with the security right you're mentioning. The only reason Domain Users have that right is because you've made them Administrators on your domain controllers.

--

Paul Adare

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