

Win2k3 Event Log and Security: Must choose between security and trustworthy

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2003-04/0266.html>

From: Jonathan Folland (jfolland.nospam@earthlink.net)

Date: 04/22/03

From: "Jonathan Folland" <jfolland.nospam@earthlink.net>

Date: Mon, 21 Apr 2003 21:45:31 -0500

When developing ASP.Net apps in Win2k I encountered an issue (many others have as well) regarding the way the EventLog.WriteEntry encounters security problems when to trying to create new Event Logs and new Event Log Sources. If the ASP.Net user is not defined as system or given Administrative rights, it cannot create the Event Log or Source and thus cannot log to the event log. There have been a number of responses placed on various news groups. In opinion, none of these responses adequately address the issue.

The responses I have encountered include:

1) Write a Program to create the event log and its sources in the registry. Run this program under a user account that has administrative privileges.

In my opinion, this is not a very good solution. What happens if a developer fumble fingers the name of the event log or its source or during coding of the application developers create new sources. In order for this to be effective, someone would need to write a program that scanned all source code for methods of New EventLog and WriteEntry, then parse the method arguments to come up with a comprehensive list of Logs and Sources. How many development shops are going to do this so that they can write to the event log?

2) Change the userName attribute in the processModel key in machine.config to SYSTEM.

First, I am not entirely certain of the security impact of doing this. I am guessing that it is not the wisest thing to do. Regardless, this did not work on the Win2K3 Server machine I am using.

3) Give the ASP.Net user Administrative privileges on the machine.

Clearly this represents a security problem. However, it works on Win2k, but not on Win2k3.

4) Under Win2k3, change the identity under which the default application pool runs from the I_WAM account to System account.

This is clearly a security problem, but it solves the problem of being able to reliably write to the event log.

The above solutions are the only ones that I have encountered to potentially solve this problem. I believe that developers must be confident that when they attempt to write to the event log, that the entry will be made. In my opinion, this is an absolutely critical item for "trustworthy" computing. Solution 1 does not present a security problem, but it presents a reliability problem. The remaining solutions are all security problems. Thus, in my opinion, developers are faced with developing apps that are either not secure or not reliable.

First, I am hoping that someone can respond to this with a good solution that solves my predicament. Second, if no reasonable solution is supplied, I am hoping that Microsoft will "own up" to this issue by creating a hot fix for this. Finally, (the black mail part), if neither of these occur, I am going to post this on every news group I can find until Microsoft addresses the issue effectively, because to be quite honest, I am ticked off that I even have to write this.

Jonathan Folland
jfolland@no-spam.telesightcommerce.com.no-spam