

iis 6 exception issue

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2005-02/0063.html>

From: James Perks (jperks_at_itchannel.net)

Date: 02/02/05

Date: Wed, 2 Feb 2005 17:16:04 -0000

Hi there,

We have a customer who is experiencing several issues after migrating their site from iis 5 to 6. Below is the customer's description of the problem.

>From the surface it appears like it is a permissions problem and this would make sense due to the security changes in iis 6 compared to 5.

I have asked for auditing to be turned on to detect if there is a file permissions problem and am still waiting for this information.

The confusing fact is the spawned exe seems to be running in the context of the domain service account (from task manager), and should have access to the file system.

I have found within the 06_CHAPTER_3_Securing_Web_Sites_and_Applications.doc under the section 'Identifying the Impersonation Behavior for ASP Applications' that

If an authenticated user makes a request, the thread token is based on the authenticated account of the user.

Therefore I would suspect the exe would be launched in the context of the authenticated user.

Regards

James Perks

Running a 'classic' ASP application on Windows server 2003 web edition.

To try and describe the problem succinctly:

Background:

The asp application launches an executable on the web server (asynchronously) – which in essence writes to a text file.

The web site is set to use NTLM authentication.

The web site runs under a custom application pool with the identity of a domain service account that has permissions to run the executable (proven using the 'runas' command on the server).

Problem:

The executable runs correctly when the web page is requested by a user who has elevated privileges on the webserver (i.e. a member of the admin's

group).

The executable does not run correctly when an ordinary user requests the page.

Further information.

For each of these user scenarios, the executable appears in task manager with the correct user name (from the application domain).

When run by the ordinary user, the executable disappears too quickly and an error is written to the event log (attached).

The error occurs when the executable tries to create and write to a text file.

No errors are reported in the event log when an 'empty' executable is called by the ordinary user.

I suspect that IIS6 is launching the executable with the client's credentials, despite the service account being shown in task manager.

The problem is described exactly in this link.

<http://forum.galahtech.org/lofiversion/index.php?t10191.html>

Here is an excerpt from the application event log:

The description for Event ID (0) in Source (.NET Runtime) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. You may be able to use the /AUXSOURCE= flag to retrieve this description; see Help and Support for details. The following information is part of the event: .NET Runtime version 1.1.4322.573- ICBSDataLoad.exe - Common Language Runtime Debugging Services: Application has generated an exception that could not be handled.

Process id=0x130 (304), Thread id=0x90c (2316).

Click OK to terminate the application.