

Re: Restrict use of AMI, ADSI and WScript.Shell

Source:

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis/2004-04/1206.html>

From: George V. Reilly (george_at_reilly.org)

Date: 04/13/04

Date: Mon, 12 Apr 2004 21:26:49 -0700

Adsiis.dll and its companion, iisext.dll, lived in system32 in IIS 4.0 and 5.x, but moved to system32\inetsrv for IIS 6.

```
--
Liberty means responsibility. That is why most men dread it.
-- George Bernard Shaw
(Get Witty Auto-Generated Signatures from http://SmartBee.org)
George V. Reilly george@reilly.org
"Peter Johansen" <peterJohan13384@hotmail.com> wrote in message
news:5CJec.140611$Bk31.70372@twister01.bloor.is.net.cable.rogers.com...
> Hi David,
>
> Thank you very much. I'm really glad it's as simple as setting NTFS
> permissions on the 2 files you mentioned. Just a note - the "adsiis.dll"
was
> in the "%windir%\system32\inetsrv" folder on my server, not the
> "%windir%\system32" folder. Not sure if different Windows versions has the
> file in different places but thought I should mention it in case someone
> else ever has the same Q's. I assume it's the same file though.
>
> If anyone has any suggestions as to what other dangerous objects should be
> restricted in this manner I would appreciate it. The one possible security
> risk I will have to allow unfortunately is access to the FSO, but I think
I
> have that locked down fairly well since I'm using different IUSR's and app
> pool identities for each web site, with appropriate NTFS permissions set
on
> the web root and contents.
>
> Thanks!
>
>
> "David Wang [Msft]" <someone@online.microsoft.com> wrote in message
> news:ufclRcQIEHA.4092@TK2MSFTNGP11.phx.gbl...
> > You can use Filesystem ACL on %windir%\System32\wshom.ocx to control
who
> > can create the WScript.Shell object (as well as all the WScript.*
objects)
> > in one shot. Can't use Filesystem ACL to allow one users to create
> > WScript.Network but not WScript.Shell, for example.
> >
> > I'm not certain if ADSI has anything comparable to WMI, but you can use
> > the
> > same Filesystem ACL approach on %windir%\system32\adsiis.dll to prevent
> > users to access all of the IIS:// ADSI namespace.
```

microsoft.public.inetserver.iis: Re: Restrict use of AMI, ADSI and WScript.Shell

```
> >
> > --
> > //David
> > IIS
> > This posting is provided "AS IS" with no warranties, and confers no
> rights.
> > //
> > "Peter Johansen" <peterJohan13384@hotmail.com> wrote in message
> > news:ZFFec.132167$Bk31.35595@twister01.bloor.is.net.cable.rogers.com...
> > Hi, I would appreciate any tips on restricting WMI, ADSI, and
> WScript.Shell
> > from being used in ASP pages by anyone other than the Administrators
group
> > in a shared hosting environment. WMI seems like it can be restricted
> fairly
> > easily via the "WMI Control" MMC snap-in. But how about ADSI and
> > WScript.Shell? This is for IIS 6.0 on W2K3.
> >
> > By the way, each web site has it's own IUSR account and application
pool.
> > The application pool's identity is also a unique user account for each
> web.
> > This allows me to restrict access to files between different webs.
> However,
> > I would still like to restrict WMI, ADSI and Wscript.Shell from being
used
> > at all, except by the Administrators group.
> >
> > Thanks for any tips and advice.
> >
> >
> >
> >
> >
> >
> >
```