

Re: how to block/disable windows scripting host ?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2004-03/0300.html>

From: David Wang [Msft] (*someone_at_online.microsoft.com*)

Date: 03/10/04

Date: Wed, 10 Mar 2004 14:31:48 -0800

It is not possible to declaratively "disable" arbitrary objects on a per site basis.

However, I can think of a hack which may work for you, using filesystem ACLs. ACL the DLL implementing the WSH objects to be inaccessible to the remote authenticated user from IIS.

I have attached a recent post showing how to selectively block certain websites (but not others) from using the FSO object. WSH objects are implemented by another binary, so apply the same logic. It definitely works on IIS6; on other IIS versions, under some configurations, it may not be possible -- but you haven't given any information on your configuration so I cannot advise further.

--

//David

IIS

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

//

"Akhlaq Khan" <akhlaq.khan@softechww.com> wrote in message news:eVrN2\$rBEHA.2404@TK2MSFTNGP11.phx.gbl...

hi,

can u please tell me how can i block WSH scripts and wscript.shell objects from being created in ASP pages ?

one of my servers recently got hacked and i am desparately looking for a solution.

thanks,

akhlaq.

"Leythos" <void@nowhere.com> wrote in message news:MPG.1a886bc34f9beb9c98a130@news-server.columbus.rr.com...

> In article <844101c3e9b3\$3fb2dc10\$a101280a@phx.gbl>,

> dylanmilks@yahoo.com says...

> > Through my ASP app, I'm using wshell.script to open a cmd

> > window. If I don't pass any parameter to cmd, it works

> > fine. If I try to give it some parameters, it gives

> > me "access is denied".

> >

> > This works:

> > Set oShell = Server.CreateObject("WScript.Shell")

> > Set oExec = oShell.Exec("cmd /c")

> >

> > This returns access denied:

> > Set oShell = Server.CreateObject("WScript.Shell")

> > Set oExec = oShell.Exec("cmd /c dir c:\")

microsoft.public.inetsrvr.iis.security: Re: how to block/disable windows scripting host ?

```

> >
> > Any idea why?
> > How can I get this to work?
>
> You don't want to let it work - IIS should NOT be able to access CMD at
> any time, you will be hacked.
>
> --
> --
> spamfree999@rrohio.com
> (Remove 999 to reply to me)

```

```

begin 666 Re_Disabling FSO in certain websites.nws
M1G)O;3H@(D1A=FED(=%A;F<@6TUS9G1=(B \<V]M96]N94!O;FQI;F4N;6EC
M<F]S;V9T+F-O;3X-"E)E9F5R96YC97,Z(#PR-V5A9&,V8RXP-# R,C@R,#$V
M+C,T-64Q8C=C0'!O<W1I;F<N9V]O9VQE+F-O;3X-"E-U8FIE8W0Z(%)E.B!$
M:7-A8FQI;F<@1E-/(&EN(&-E<G1A:6X@=V5B<VET97,-"D1A=&4Z(%-A="P@
M,C@&1F5B(#(P,#0@,C,Z,C$Z,34@+3 X,# -"DQI;F5S.B T, T*6"U0<FEO
M<FET>3H@,PT*6"U-4TUA:6PM4')I;W)I='DZ($YO<FUA; T*6"U.97=S<F5A
M9&5R.B!:-:6-R;W-O9G0@3W5T;&]O:R!%>'!R97-S(#8N,# N,C@P,"XQ,34X
M#0I8+4UI;65/3$4Z(%!R;V1U8V5D($)Y($UI8W)O<V]F="!-:6UE3TQ%(8V
M+C P+C(X,# N,3$V-O T*365S<V%G92U)1#H@/"-(539N87 D1$A!+C(Q.#!
M5$LR35-&$Y'4# Y+G!H>"YG8FP^#0I.97=S9W)O=7!S.B!M:6-R;W-O9GON
M<'5B;&EC+FEN971S97)V97(N:6ES+G-E8W5R:71Y#0I.3E10+5!O<W1I;F<M
M2&]S=#H@=&ED93$P."YM:6-R;W-O9GON8V]M(#(P-RXT-BXR,C@N,38-"E!A
M=&@Z(%1+,DU31E1.1U P."YP:'@N9V)L(51+,DU31E1.1U P.2YP:'@N9V)L
M#0I8<F5F.B!42S)-4T943D=0,#@N<&AX+F=B;"!M:6-R;W-O9GON<'5B;&EC
M+FEN971S97)V97(N:6ES+G-E8W5R:71Y.C(Y.3$Q#0H-"DET(&ES(&YO="!P
M;W-S:6)L92!T;R!D96-L87)A=&EV96QY(")D:7-A8FQE(B!A<F)I=')A<GD@
M;V)J96-T<R!O;B!A('!E<@T* <VET92!B87-I<RX-"@T*2&]W979E<BP@22!C
M86X@=&AI;FL@;V8@82!H86-K('=H:6-H(&UA>2!W;W)K(&9O<B!Y;W4L('5S
M:6YG(&9I;&5S>7-T96T-"D%#3',N("!"87-I8V%L;'DL('EO=2!S970@=7 @
M=&AE('=E8G-I=&5S('1H870@:&%V92!&:6QE4WES=&5M3V)J96-T#0ID:7-A
M8FQE9"!T;R!A;'=A>7,@97AE8W5T92!W:71H(&$@8V5R=&%I;B!U<V5R(&ED
M96YT:71Y("AF;W(@8V]M<&QE=&5N97-S+"!)#0IW;W5L9"!L;V-K(&)O=&@@
M=&AE(%!R;V-E<W,@261E;G1I='D@87,@=V5L;"!A<R!U<V5R(&ED96YT:71Y
M('10('!H:7,@=7-E<@T* <V\@=&AA="!P96]P;&4@9&]N)W0@:&]P(&%R;W5N
M9"!I="!W:71H(% )E=F5R=%1O4V5L9B@I("D@86YD('1H96X@<&AY<VEC86QL
M>0T*04-,('1H92!F:6QE(&EM<&QE;65N=&EN9R!38W)I<'1I;F<N1FEL95-Y
M<W1E;4]B:F5C="!T;R!D96YY(&%C8V5S<R!T;R!T:&%T#0IU<V5R+B @1&]I
M;F<@=&AI<R!D;V5S(&YO="!A9F9E8W0@=&AE(&%C8V5S<R!O9B!A;GET:&EN
M9R!E;'=E('1H870@;F5E9',-"D933R M+2!O;FQY('1H92!&4T\@871T96UP
M=',@9G)O;2!T:&]S92!S<&5C:69I8R!W96)S:71E<RX-"@T*5&AI<R!H86-K
M('=O;B=T('=O<FL@:68@>6]U(&-A;FYO="!C;VYT<F]L('1H92!U<V5R(&ED
M96YT:71Y(&]F('EO=7(@=7-E<G,L#0IB=70@22!S=7-P96-T('EO=2!S:&]U
M;&0@:&%V92!T;&ES('5N9&5R(&-O;G1R;VP@:68@>6]U(&%R92!A(&AO<W1E
M<BX-"@T*4V\L('=H870@>6]U('=O=6QD(&1O(&ES.@T*,2X@0W)E871E(&%N
M($%P<%!O;VP@=VET:"!A(&-U<W1O;2!U<V5R(&ED96YT:71Y(&]F($1E;FEE
M9$933U5S97(-"C(N(%-E="!A;&P@=V5B<VET97,@=&\@=7-E('!H:7,@07!P
M4&]O;"!I9B!Y;W4@=VES="!T;R!D96YY('1H96T@1E-/(&%C8V5S<PT*,RX@
M4V5T(&%N;VYY;6]U<R!U<V5R(&ED96YT:71Y('1O(&)E($1E;FEE9$933U5S
M97(@9F]R(&%L;"!W96)S:71E<R!I;B C,@T*-"X@4V5T($1E;GD@4F5A9"]%
M>&5C=71E($%#3"!O;B!T:&4@9FEL92!I;7!L96UE;G1I;F<@1E-/( "AM:6YE
M('=A>7,-"G-C<G)U;BYD;&PI(&9O<B!$96YI961&4T]5<V5R#0HU+B!)9B!T
M:&5S92!W96)S:71E<R!H879E(&%U=&AE;G1I8V%T:6]N+!"!Y;W4@;6%Y(&YE
M960@=&\@861D('!H;W-E('5S97)S(&%S#0IW96QL('1O('1H92!$96YY(% )E
M860017AE8W5T92!!0TP@*&]R('5S92!A(&=R;W5P(&9O<B!T:&ES*0T*#0HM
M+2 -"B\O1&%V:60-"DE)4PT*5&AI<R!P;W-T:6YG(&ES('!R;W9I9&5D(")!
M4R!)4R(@=VET:"!N;R!W87)R86YT:65S+"!A;F0@8V]N9F5R<R!N;R!R:6=H
M=' ,N#0HO+PT*(F]M87(@:V]U9'-I(B \;VUA<FM :F5E<F%N+F-O;3X@=W)O
M=&4@:6X@;65S<V%G90T*;F5W<SHR-V5A9&,V8RXP-# R,C@R,#$V+C,T-64Q
M8C=C0'!O<W1I;F<N9V]O9VQE+F-O;2XN+@T*5VEN,FLS+TE)4S8-"@T*22!W
M;W5L9"!L:6ME('1O(&1I<V%B;&4@=&AE(&9I;&4@<WES=&5M(&]B:F5C="!F

```

microsoft.public.inetsrvr.iis.security: Re: how to block/disable windows scripting host ?

```
M;W(@<V]M92!O9B!T:&4@<VET97,-"G1H870@:6T@:&]S=&EN9R!O;B!M>2!S
M97)V97(@9F]R('E8W5R:71Y(')E87-O;G,L('O('1H:7,@<VAO=6QD;G0@
M8F4-"F$@<V5R=F5R('=I9&4@<V]L=71I;VXN#0H-"DED(&%P<')E8VEA=&4@
186YY('!O:6YT97)S+ T*#0H`
`
```

end