

Re: CGI can't spawn process under IIS6

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2004-08/0138.html>

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

Date: 08/07/04

Date: Sat, 7 Aug 2004 01:00:45 -0700

You do not need to change the ACL on CMD.EXE to spawn new processes --- instead of calling system(), call CreateProcess() with the EXE filename directly, and this will launch that EXE without using CMD.EXE to execute it --- so you do not need to weaken ACLs on CMD.EXE.

In any case, what has happened with Windows Server 2003 and IIS6 is that all the console commands (like cmd.exe) have been ACL'd to be inaccessible to IIS users unless they are authenticated administrator (that's why when you put IUSR in Administrators, it worked). Thus, you should consider any code that require giving anonymous user access to CMD.EXE as exposing a security vulnerability.

Your workaround is actually ineffective. Hiding CMD.EXE but still placing it on the PATH means anyone just has to execute "cmd" to run it from wherever you hid it --- even easier to hack. Only secure method is to keep CMD.EXE inaccessible to IIS users.

```
--
//David
IIS
This posting is provided "AS IS" with no warranties, and confers no rights.
//
"Michael" <soolkin@icentrix.com> wrote in message
news:7b9f3f2c.0408030624.385950cf@posting.google.com...
Paul Lynch <paul.lynch@nospam.com> wrote in message
news:<ivlug0l2s8lbj22fvuvvml04qsi44hf6t5@4ax.com>...
> On 2 Aug 2004 13:54:28 -0700, soolkin@icentrix.com (Michael) wrote:
>
> >Hello gurus,
> >
> deleted
> >Thank you
> >Michael
>
> Michael,
>
> This behaviour is by default in IIS6 as part of the 'locked down' mode
> of installation. Its good practice really, you wouldn't actually want
> non-privileged users to have access to programs in the system root
> directory would you ?
>
> If you do then you have to explicitly grant the permissions to the
> account in question.
```

microsoft.public.inetserver.iis.security: Re: CGI can't spawn process under IIS6

>
> PRB: IIS 6.0: CGI Code That Calls External Applications May Fail
> <http://support.microsoft.com/?id=311481>
>
>
> Regards,
>
> Paul Lynch
> MCSE
Thanks a lot Paul,
I've learned it yesterday, that I've got to change the permissions on
cmd.exe...
I don't like doing it, but what is the alternative? I need to run some
executables from within a page. Right now it's email sending exe,
later more and more...
I was exploring possibility of prepending PATH environment variable
for IUSR_ with some hidden location where I could store my copies of
executables and cmd.exe with permissions granted... Than I wouldn't
need to touch anything in system32. No luck so far...
Thanks again,
Michael Soolkin