

## Re: SSL 2.0

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2008-01/msg00025.html>

---

- *From:* David Wang <[w3.4you@xxxxxxxxxx](mailto:w3.4you@xxxxxxxxxx)>
  - *Date:* Fri, 11 Jan 2008 12:50:59 -0800 (PST)
- 

Yes, this is the classic tradeoff between compatibility and security.

Believe me, the value of just about every single one of those settings had a heated discussion (which is unfortunately not publicized anywhere) between securing defaults and breaking people on upgrade vs leaving defaults for people to tweak.

Basically, all the settings have gone through review of being "secure by default" and teams have to provide rationale for anything perceived as insecure -- usually a calculated risk-tradeoff for compatibility.

I suspect that the argument for SSL2 would have focused on the fact that SSL3 would be chosen "by default" by most browsers and that users who are using SSL2 have been doing so on their own choice for some time now -- so it does not warrant changing the default value for SSL2 at all.

Now, you may view this as a security risk since the defaults are not secure, but in reality the product team views this as a very reasonable tradeoff between security and compatibility. The resulting behavior is that no one is accidentally using SSL2 (so no security risk) while those intentionally use SSL2 are not broken on upgrade. A sort of "best of both worlds" compromise.

Yes, this compromise will never satisfy the ideological zealot which wants "secure defaults", but consider this -- it may not be worth it to anger 80% of users broken by an upgrade to satisfy the zeal of 20% of users. Always keep this in mind.

Now, the decision is always case-by-case -- I'm just giving you the rationale where compatibility wins over changed secure defaults -- but most of the time in Windows Server 2003 breaking security changes were made.

I understand your expectation that if a serious flaw is found in SSL3 that you'd expect it to be disabled by default, but believe me there would be a big discussion in Microsoft about changing that default -- it is unfortunate that you never see the passionate arguments on both

Re: SSL 2.0

sides for the change — you only see the end result and think either "yes, Microsoft secured the default" or "Microsoft screwed up security by default \*again\*" — most choices are simply not as easy as you think, and it is hard to please everyone regardless if you give them a choice or not.

Regarding the SSL selection UI in IIS — that is a good idea, but there are several problems with such a proposal such that it will likely never happen. You are asking the IIS team to take responsibility to make/depend on an UI provided by the SCHANNEL team to introduce knobs into the IIS UI which make little difference to 90+ % of users. By definition, such configuration do not get prime treatment in the UI and go to the registry — where those that care about security can tweak to their hearts content. Basically, I do not see giving the 1% user preferential treatment in the UI to override secured defaults in the OS and confusing the other 99% user to be a good idea.

Remember, proper UI design is not about giving access to all the choices — it is about giving access to the \*right\* choices. Balancing security, compatibility, and usability is HARD, especially for a widely used product like IIS.

//David  
<http://w3-4u.blogspot.com>  
<http://blogs.msdn.com/David.Wang>  
//

On Jan 11, 6:55 am, Smurfman <smurf...@xxxxxxxxxxxxxxxx> wrote:

David thanks for your input on this. I appreciate your time, and what you are saying.

One might argue then, why make the OS change in this case to disable PCT 1..0 by default from Windows 2000 Server to Windows 2003 Server. Again, if SSL 2.0 according to all the security experts is not good and is not secure, then again, why not disabled it by default in Windows 2003 Server and KB would read, hey if you have old web server software that needs to use SSL 2.0 then you will need to enable the protocol – otherwise users will not be able to connect. The idea I guess would be to harden the Default install – or a service pack that would do this for you, rather than have someone find that SSL 2.0 was being allowed.

I get what you are saying and true there is no perfect world. But lets face it, in reality why do we have to keep poking around in the registry and

Re: SSL 2.0

adding keys and changing things to make something secure. Why not patch IIS to have a box that tells me what protocols within SSL I want to accept. And true if in 2013 there was a serious flaw found in SSL 3.0 and in 2014 – Windows 2014 Server was release I would expect that the SSL 3.0 would be disabled by default.

Long and short of it, was unless I read this KB, I guess I wouldn't have know about PCT.

I appreciate your input...

So that leaves me with – how do I test to see if SSL 2.0 is disabled or PCT when attempting to hit my web server?

Thanks

"David Wang" wrote:

Default values are all defined in source code. They may not be published, but not because of nefarious reasons.

For example, do you want Microsoft to publish a list of the millions of "default" values for every single possible configuration switch in Windows every time it ships a service pack? Does that even make sense? But if Microsoft does not publish such a list, users can complain that Microsoft is abusing its market position and withholding information. See how users frequently paint things into a lose-lose situation? They just want want want, even if they cannot use it.

As for why disabling some behaviors require setting Enabled=0 while others are disabled by default and do not require such configuration settings, here is one possible explanation which stems naturally from software development.

<HYPOTHETICALLY>

Suppose in 2008 we have a feature SSL3 which is enabled by default and SSL3.5 which is disabled by default in SCHANNEL because it conflicts with SSL3 and is not yet popular. Now, fast forward to 2015, when SSL4 is introduced to be on by default because someone discovered a severe security flaw in SSL3 in 2013.

## Re: SSL 2.0

What would the corresponding KB entry say?

To disable SSL3, you must set Enabled=0 in the registry.

To disable SSL3.5, you do nothing since it was disabled by default.

Now, you may argue "why not change the default value of SSL3 to be disabled instead of requiring the user to set Enabled=0 in the registry", but that's the problem with defaults. Some customer may have purchased fixed systems in 2010 that only used SSL3 (which was still viable at the time), and changing the default to disabled will simply break those systems on upgrade UNLESS they remember to add the Enabled=ffffffff registry key. How would you like it if on upgrades Windows requires you to tweak 100 different values just to keep your software functional? Hindsight is 20/20. Who knew in 2010 that SSL3 would be insecure?

Of course, if the default value of SSL3 is left alone, a user in 2015 may look at the instructions for disabling SSL3 and SSL3.5 and say "hmm, I would have expected to find a similar key already present in the SSL3.5 protocol if Windows 2015 Server is disabled [SSL3] by default".

Now, another school of software design would have said "fill the Registry with the current "default values" for each configuration switch", so users can tell which are on and off by default and everything looks congruent. While this design is open and leaves nothing to question, it does not resolve the problem of "changing default values" and only introduces legacy support costs for Microsoft to maintain those values for the OS. As anyone in the software business would agree, you want to introduce as little legacy as possible to minimize support costs, so in terms of the costs of a design choice, "hidden defaults" wins over "public defaults".

Note that this design choice is opposite of Open Source, which due to its indifference of support costs (the user is responsible for support — go read the source code), it favors verbose configuration files and public default values along with access to source code so that the user can figure it out.

Re: SSL 2.0

Is one necessarily better than the other? Not really. It all depends on the user. For the casual user, too many choices is dangerous. For the tinkerer, there are never enough choices.

//David  
<http://w3-4u.blogspot.com>  
<http://blogs.msdn.com/David.Wang>  
//

On Jan 10, 1:52 pm, Smurfman <smurf...@xxxxxxxxxxxxxxxx> wrote:

Okay, I think I get what you are trying to say –

However, if the KB is telling me to disable for example SSL 2.0 to ADD a DWORD called Enabled and assign it a value of 0x00000000 (0) to disable the SCHANNEL protocol I would have expected to find a similar key already present in the PCT 1.0 protocol if Windows 2003 Server is disabled by default.

In addition, ALL of the protocol values for default are not defined (value not set)

Just want to make sure I am understanding the KB correctly.

How would preform a PCT 1.0 test? I can see where I can test the SSL 2..0 / 3.0 and TLS 1.0 in the Internet Explorer browser advanced settings... but don't know how I might be able to do this for the PCL to see if in fact it is disabled

Thanks

Re: SSL 2.0

"David Wang" wrote:

When you use the Windows API to read Registry keys, there is a "default" value that is provided when the key does not exist.

Thus, the KB article is telling you that when there is no key, the default value is disable (0).

How does one know if PCT is disabled by default? You either trust the KB article or do your own test.

Can you clarify your question.

//David  
<http://w3-4u.blogspot.com>  
<http://blogs.msdn.com/David.Wang>  
//

On Jan 10, 8:09 am, Smurfman  
<smurf...@xxxxxxxxxxxxxxxx> wrote:

In reading KB 187498 – I found a string that stated by default PCT is not enabled on Windows 2003 Server.

However when I look at the key location as outlined in the KB

Re: SSL 2.0

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL\1.0\Server

There is no values for the Enabled DWORD

Enabled with a DWORD value of 0x00000000 is disabled and 0xffffffff is enabled according to KB 216482 –

So – since the value is not present by default, how is it that PCT is disabled by default according to the aforementioned KBs?

Thanks

""WenJun Zhang[msft]"" wrote:

No, Microsoft hasn't suggested to enable SSL 3.0 only and disable all the other ciphers. Only SSL 2.0 is not recommended for sure. The answer of your question is

Re: SSL 2.0

fully based  
on your real  
scenario. If  
your web  
application  
has  
quite  
critical  
concern on  
the security  
and  
consider  
only SSL  
3.0 clients  
should be  
allowed to  
access the  
site, then I  
believe it's  
fine to  
disable  
the other  
ones.

Furthermore,  
TLS 1.0 and  
SSL 3.0 are  
quite  
similar  
protocols.  
You may  
look  
through the  
following  
article:

What is  
TLS/SSL?

<http://technet2.microsoft.com/windowsserver/en/library/ed5ae700-e036-45795dbb99a21033.mspx?mfr=true>

Hope the  
info will be  
of some  
help. Have

Re: SSL 2.0

a nice day.  
:-)

Sincerely,

WenJun  
Zhang

Microsoft  
Online  
Community  
Support

=====  
Get  
notification  
to my posts  
through  
email?  
Please refer  
to:

<http://msdn.microsoft.com/subscriptions/managednewsgroups/default.aspx>  
ications.

Note: The  
MSDN  
Managed  
Newsgroup  
support  
offering is  
for  
non-urgent  
issues  
where an  
initial  
response  
from the  
community

Re: SSL 2.0

or a  
Microsoft  
Support  
Engineer  
within 1  
business  
day is  
acceptable.  
Please note  
that each  
follow  
up response  
may take  
approximately  
2 business  
days as the  
support  
professional  
working  
with you  
may need  
further  
investigation  
to reach the  
most  
efficient  
resolution.  
The  
offering is  
not  
appropriate  
for  
situations  
that require  
urgent,  
real-time or  
phone-based  
interactions  
or complex  
project  
analysis and  
dump  
analysis  
issues.  
Issues of  
this nature  
are best  
handled  
working  
with a  
dedicated

Re: SSL 2.0

Microsoft  
Support  
Engineer by  
contacting  
Microsoft  
Customer  
Support  
Services  
(CSS) at:

<http://msdn.microsoft.com/subscriptions/support/default.aspx>.

=====

This posting  
is provided  
"AS IS"  
with no  
warranties,  
and confers  
no rights.–  
Hide quoted  
text –

– Show quoted text — Hide  
quoted text –

– Show quoted text — Hide quoted text –

– Show quoted text –