

## Re: Compromise?

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2003-12/0099.html>

---

**From:** Stephen Dybing [MSFT] ([stephd\\_at\\_online.microsoft.com](mailto:stephd_at_online.microsoft.com))

**Date:** 12/03/03

Date: Wed, 3 Dec 2003 12:31:05 -0800

Yes, if you don't provide a password on your SA account, anybody able to run "OSQL /Usa /P /S<servername>" (or any other client program of their choice) and connect now has complete control over your SQL Server. And on top of that, that person now has whatever permissions that the account running SQL Server has (because of xp\_cmdshell). If it's a local admin, they have complete control over the box. If it's a domain admin, they have complete control over your domain. If it's a domain or local account, they have whatever permission that account has.

As you have surmised, this is a really big deal.

--

Sincerely,

Stephen Dybing

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

Please reply to the newsgroups only, thanks.

"phil b" <[anonymous@discussions.microsoft.com](mailto:anonymous@discussions.microsoft.com)> wrote in message news:018d01c3b9da\$6ecf6300\$a501280a@phx.gbl...

thanks, i appreciate your response. apology accepted.

one question lingers that seems to have been lost in all of this:

can you tell me if a blank password "sa" account, with SP3a installed and otherwise default settings, is known to Microsoft to be able to be hijacked and run a process? in other words, I don't understand what this "feature" is (meaning the ability to launch some process) and whether it is a feature to begin with.

that's really what i wanted to know. the damage is done, i'm in clean up mode, and i decided to write in case i had discovered some new flaw.

(i suppose that's why i took immediate offense, because i was only interested in informing Microsoft of a new potential flaw if it wasn't known already).

thanks,

phil

>-----Original Message-----

>OK, let me apologize for sounding condescending. I actually was attempting

>to sound confused that you didn't realize what you did.

Yeah, it sounds

>condescending in hindsight, but it really wasn't meant to.

>

>No, I do not think it is acceptable behavior, especially

## microsoft.public.sqlserver.security: Re: Compromise?

in light of our  
>company's attempts to get more secure. That's why we're  
changing the default  
>to require a strong password. As others have stated,  
that's generally the  
>way this market has behaved in the past so it really  
hasn't seemed like a  
>big deal. With all the worms and viruses hitting us  
though, that has  
>changed.  
>  
>Going back and modifying the released version of the  
software is a pretty  
>difficult operation, from what I understand. We have  
done that for the  
>Slammer fix, but apparently this hasn't made that bar as  
you've suggested it  
>should. It will be done for Yukon, however, so hopefully  
there is some light  
>at the end of the tunnel.  
>  
>Again, I'd like to apologize for my incredibly bad  
choice of phrasing...  
>  
>--  
>Sincerely,  
>Stephen Dybing  
>  
>This posting is provided "AS IS" with no warranties, and  
confers no rights.  
>Please reply to the newsgroups only, thanks.  
>"phil" <anonymous@discussions.microsoft.com> wrote in  
message  
>news:059201c3b933\$9a9f55f0\$a301280a@phx.gbl...  
>Let me say this, anyone who starts a sentence with "Uh,  
>.." means their remarks to be condescending, and so I  
will  
>respond to that attitude...  
>  
>I will gladly accept blame for leaving the front door  
>open, as you say. Perhaps you can take partial blame for  
>advertising that I have the type of house that just might  
>leave the front door open. Or one that has a default  
>lock that doesn't work.  
>  
>You actually think its acceptable behavior that a product  
>installed on an operating system can be set in a default  
>mode whereas others can use it to launch any process, at  
>will, to attack one's machine? And so you might  
>ask, "Well, what could Microsoft have done?". Well I  
>have just such an answer:  
>  
>1. It should have replaced SQL Server 2000 with a  
>revised version including all patches in SP3a, not just  
>made the patches available and advised customers to  
>install it.  
>2. And it should have included a revision making it  
>impossible to set a blank password.  
>  
>Yes, call me stupid or naïve (as you so implied), but no  
>more stupid than a manufacturer who set up their  
>customers for just such a failure, fails to correct it in

## microsoft.public.sqlserver.security: Re: Compromise?

>an acceptable way, and then tells the customer its his  
>fault.  
>  
>I love the arrogance of your response; somehow I would  
>guess Mr. Balmer or Mr. Gates might find your arrogance  
>equally amusing.  
>  
>>-----Original Message-----  
>>Uh, why the vulnerability exists? It exists because you  
>>left the front door  
>>open. In the past, it was the default account/password  
>>combination when SQL  
>>Server was installed and if your SQL Server is running  
>>under a local  
>>administrator account, you just gave anybody who has a  
>>SQL Server client  
>>tool complete control over that computer. There was a  
>>worm that hit a while  
>>back that simply scanned every machine it could find  
>>looking for SQL Servers  
>>with no password on their SA account. The only way to  
>>keep you from shooting  
>>yourself in the foot is by disallowing blank SA  
>>passwords. We're doing our  
>>best to keep you from doing that in the current  
>>versions, but we cannot  
>>remove that ability completely without breaking lots of  
>>existing  
>>applications. What we can do is warn you not to allow it  
>>and disable it by  
>>default so that you consciously have to allow the  
>>vulnerability to exist. I  
>>believe that's what we started doing with SQL Server  
>>2000 service pack 3.  
>>  
>>--  
>>I hope this makes sense,  
>>Stephen Dybing  
>>  
>>This posting is provided "AS IS" with no warranties, and  
>>confers no rights.  
>>Please reply to the newsgroups only, thanks.  
>>"phil b" <g3@philbeisel.com> wrote in message  
>>news:017301c3b90a\$371e25c0\$a401280a@phx.gbl...  
>>>  
>>> this is what happened to me. turns out that you can  
>>> be  
>>> 100% up-to-date with patches, but if the account "sa"  
>>> has  
>>> no password and the machine is exposed to the net, you  
>>> will be infected.  
>>>  
>>> nobody seems to be able to tell me why this  
>>> vulnerability  
>>> exists (because i thought a 100% patched SQL  
>>> server/system would not be able to be compromised),  
>>> but  
>>> the proof in the pudding, so to speak. perhaps their  
>>> is  
>>> a new hole. whatever.  
>>>  
>>> clear sage advice of getting the machine off the

## microsoft.public.sqlserver.security: Re: Compromise?

```
public
>>> internet and setting a password on "sa" account is the
>>> right thing to do.
>>>
>>> but i'm still wondering what this "infection" did to
my
>>> machine.
>>>
>>> there appears to be two different things that infected
>my
>>> machine in the 24 hours period when it was vulnerable.
>one
>>> created a directory of stuff under c:\winnt\system32
>>> \dllcache and ran its executables out of there. the
>>> others placed xscan.exe on my machine (and i think was
>in
>>> the process of doing more damage). somehow IRC is
>>> involved, i think as a way to find the virus' FTP
>servers
>>> or the like.
>>>
>>> the executables to look out for are: nc.exe,
>>> evntmangr.exe, identd.exe. look for any process
>running
>>> under SQL server (a tool under available via CNET
>called
>>> process explorer will give you a tree view of the
>>> processes). of course, once infected, post-reboot
>these
>>> processes will run from winlogon under svrany.exe or
on
>>> their own.
>>>
>>> symantec antivirus only said that i was infected by an
>>> IRC worm and the information they had was of limited
>>> value.
>>>
>>> if you want more information, write to me at
>>> g3@philbeisel.com. but do so soon as i will terminate
>>> this email address and the junk is starting to pile in
>as
>>> i write.
>>>
>>>
>>> >-----Original Message-----
>>> >Hello -
>>> >One of our professors is running SQL Server 2000, IIS
>>> and
>>> >VS.Net on a Windows 2000 server as part of a
>development
>>> >project for his students. I know nothing about SQL
>but
>>> I
>>> >was informed by the Network Services people that a
>>> >machine in Germany had compromised this server and
was
>>> >using TCP port 1433 to scan other networks. When I
>ran
>>> >netstat, I didn't see that connection but I did see
>>> about
>>> >one hundred connections from port 1433 to varius
```

Re: Compromise?

## microsoft.public.sqlserver.security: Re: Compromise?

```
ports
>>> on
>>> >the server from a particular subnet in Denmark. I
>>> >checked the server for vulnerabilites and found that
>the
>>> >virus protection was up to date, Windows Updates were
>>> >current and SQL SP3 was installed. According to the
>MS
>>> >SQL security site, only MS03-031 was needed. I
>>> installed
>>> >that but none of the three vulnerabilities patched by
>>> >that package seem to apply.
>>> >Port 80 and everything over port 1024 are open at the
>>> >firewall to this server.
>>> >Does it sound like this machine has been compromised
>and
>>> >if so, how can it be cleaned?
>>> >Thanks
>>> >
>>> >.
>>> >
>>
>>
>>.
>>
>
>
>.
>
```