

Re: Locked out of SBS 03

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-05/7977.html>

From: Chad A. Gross [SBS MVP] (*chad.gross_at_laytonflower.nospam.com*)

Date: 05/25/04

Date: Tue, 25 May 2004 18:41:52 -0500

Attempting that kind of change is huge . . . and even then, you couldn't completely close that backdoor. Why? The method most of these boot disks use to reset the password is to read SAM info from the disk and write a new PW for the administrator. In order to close this back door, you'd have to remove the ability to write to the SAM. Of course, we still need to write to the SAM to do minor things like add users, etc – so we couldn't unilaterally deny write access to the SAM. So what are our options? Encrypt the SAM? Ok, sure – then we get a boot disk that includes encryption-breaking algorithms . . . and admins & users start complaining about the increased processing & network overhead, longer login times, etc . . .

I'm sorry, but if the ability to reset the Admin password w/ a boot disk is what allowed a system to be compromised, then your security broke down so many places it isn't funny. That's like demanding a better jewelry box lock because your wife's diamonds were stolen from a small jewelry box you kept in a safe in your home that was locked down with the security system set and a very unsociable canine at home. The burglar got by the dead bolts, alarm, mad dog & safe – but if that jewelry box lock had only held . . .

Let's face it – in the SMB space, if someone really wants into our server, they're most likely going to get in one way or another. The only truly secure computer is the PC that is turned off. Period. Assess your risks, and take the necessary steps to provide yourself with a reasonable level of protection. Yes there are back doors. There are back doors with every OS. You're more likely to get 100% uptime (screw five 9's) or discover perpetual motion before you'd get a truly bullet-proof OS . . .

--

Chad A. Gross - SBS MVP
SBS ROCKS!
www.msmvps.com/cgross
www.gosbs.org
Jeff L wrote:

> Mike,
>

> I am glad you know how to jumper the bios as well. Still looking for
> some advice that would stop this functionality for admin password
> reset. I don't need advice on physical security. Never once said it

microsoft.public.windows.server.sbs: Re: Locked out of SBS 03

> was an issue.
>
> Physical security can be compromised. The admin password reset is a
> huge hole. There has to be a way to wrap a .dll or something so that
> this can be cut off.
>
> Here is the question: How do you cut off access to Admin Password
> Reset tools?
> Maybe I should repost it.
>
> Regards,
> Jeff Loucks
> Available Technology ®
> Solutions For Professionals ®
> www.availbletechnology.com
>
>
> "Mike R" <research@rollesolutions.com> wrote in message
> news:OmqKS9mQEHA.3300@TK2MSFTNGP09.phx.gbl...
>> Hey Jeff,
>>
>> I don't think you could do it if you wanted to (remove access to
>> admin pass reset). The tools that I use are created for people that
>> have a real problem, they have inadvertently locked themselves out
>> of their server. You use it by starting setup (for whatever OS it
>> is) and hitting F6 when it asks if you need to load additional
>> drivers. Once that is done it pops right into a screen that allows
>> the administrator password to be reset.
>> As many have already mentioned, you shouldn't have to worry about
>> this if physical access is not possible by anyone other than
>> yourself and those you trust (and have a reason to have access).
>> Your bios password does absolutely nothing for you as it can be
>> reset in a matter of seconds by simply swapping a jumper on the
>> motherboard for a few seconds.
>> Best of luck to you...
>>
>>
>> "Jeff L" <newsgroupsremoveandunderscore_jeff@availabletech.net>
>> wrote in message news:%23g0u4bmQEHA.2572@TK2MSFTNGP12.phx.gbl...
>>> Thanks Susan,
>>>
>>> I am on top of the physical security issue but my question was not
>>> about physical security. I am aware of removing drives and gaining
>>> access to the data. We can and have protected against that.
>>>
>>> We have also changed the bios to password protected and removed the
>>> removable media drives from the boot order.
>>>
>>> I could get past all of that so how do I remove access to admin
>>> password reset? Anyone know how to do that?
>>>
>>> Feel free to contact me directly if you do not want to post it.
>>>
>>> Regards,
>>> Jeff Loucks
>>> Available Technology ®
>>> Solutions For Professionals ®
>>> www.availbletechnology.com
>>>
>>>
>>> "Susan Bradley, CPA aka Ebitz - SBS Rocks [MVP]"
>>> <sbradcpc@pacbell.net> wrote in message

microsoft.public.windows.server.sbs: Re: Locked out of SBS 03

```
>>> news:##kXjNmQEHA.568@TK2MSFTNGP12.phx.gbl...
>>>> Any operating system is vulnerable to physical access. Microsoft
>>>> didn't put it there. I can do likewise with any operating system.
>>>> If I can physically remove a harddrive and the data is not
>>>> encrypted, I can get to that data. Simple as that. If I have
>>>> access to that drive, it's mine.
>>>>
>>>> Put a lock on the door of the computer room.
>>>> A lock on the floppy drive.
>>>>
>>>> This isn't a trick. When WinXP could be "hacked" by using a Win2k
>>>> cdrom and booting from that and oh horrors you could reset the
>>>> admin password in that manner, the security community went... ho
>>>> hum... yeah? So? Call me with a real security issue. One that can
>>>> be hacked remotely.
>>>>
>>>> Physical security dude. Basic rules of security is restrict
>>>> physical access.
>>>>
>>>> Jeff L wrote:
>>>>> I would prefer to see that backdoor closed.
>>>>>
>>>>> I used to have a tech that worked for me that knew all those
>>>>> tricks, I had forgotten about them. My bad... I would prefer
>>>>> there not be a backdoor and those who make mistakes have to do
>>>>> more work then those who plan.
>>>>>
>>>>> I agree with the physical security thing but I don't like
>>>>> Microsoft leaving a backdoor open.
>>>>>
>>>>> Anyone know how this works, what the source of the change is? Is
>>>>> there
>>>>> a
>>>>> way
>>>>> to protect against it?
>>>>>
>>>>> Thanks,
>>>>> Jeff
>>>>>
>>>>> "Jeff L" <newsgroupsremoveandunderscore_jeff@availabletech.net>
>>>>> wrote in message news:#hSTysdQEHA.2452@TK2MSFTNGP11.phx.gbl...
>>>>>
>>>>>> I am very unhappy to see that!
>>>>>>
>>>>>> How do I protect against this type of hack!
>>>>>>
>>>>>> "Mike R" <research@rollesolutions.com> wrote in message
>>>>>> news:O#uEMWdQEHA.3744@TK2MSFTNGP10.phx.gbl...
>>>>>>
>>>>>>> go to www.lostpassword.com and get passware kit. It's expensive
>>>>>>> but
>>>>>>>
>>>>>>> allows
>>>>>>>
>>>>>>>> you to reset the admin password. Keep it in a safe place so
>>>>>>>> other users can't get to it.
>>>>>>>>
>>>>>>>>
>>>>>>>>> "John L" <anonymous@discussions.microsoft.com> wrote in message
>>>>>>>>> news:A1BD6AFB-4189-494E-8B28-CA7F24CA0ABF@microsoft.com...
>>>>>>>>>
>>>>>>>>>> I got a new SBS 2003 server, while doing the intial setup I
```

