

## Re: Messenger Service

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-11/2218.html>

---

**From:** Kevin Davis<sup>3</sup> (zkevindavisz\_at\_cfl.rr.com)

**Date:** 11/29/03

Date: Sat, 29 Nov 2003 05:23:36 GMT

On 28 Nov 2003 10:04:05 -0800, levinson\_k@despammed.com (Karl Levinson [x y] mvp) wrote:

>Kevin Davis<sup>3</sup> <zkevindavisz@cfl.rr.com> wrote in message  
news:<m7bdsvkt6o5967bqs1dvu1ukjcrh5rm0c6@4ax.com>...

>

>> What is unwise from a security standpoint is to run any services that  
>> are not needed. If you don't need the Messenger Service, disable it.  
>> if you need it, keep it running but be aware that it has a serious  
>> vulnerability that needs patched immediately.

>

>> What is also unwise from a security context is to use something as a  
>> security tool that was never intended to be that. To use the  
>> Messenger Service as an IDS of sorts for warning you that your  
>> firewall is down is bad. If you need an IDS system to alert you to  
>> intruders, run a real one. There is a free open source one called  
>> Snort that would do the trick.

>

>What you say is not exactly untrue, but for most home users, hardening  
>a computer by disabling services and a long list of other things  
>manually is usually not the ideal answer, due to the time and  
>expertise necessary and the likelihood that mistakes will be made.  
>While it is true that firewall plus disabling services is more secure  
>that just firewall alone, for most home users, firewall should be the  
>first step, disabling the messenger service and Snort for IDS are  
>optional ninth and tenth steps.

I absolutely agree. Firewall first. Absolutely. Do the others as time and expertise allows.

>

>Snort is a fine IDS, but there are a lot of other things that were  
>never meant to be IDS that are nevertheless good to monitor for signs  
>of intrusion, such as the Windows System and Application logs,  
>computer reboots, service starts and stops, file changes, IIS logs,  
>router syslogs, local user databases, windows file access auditing on  
>key files, etc.

I would take issue with the idea that the logs were never meant to monitor for signs of intrusion. I would contend that the logs are there for a variety of reasons. One being providing evidence of intrusion. The logs also are much more benign. They don't open a possible port of entry up to be exploited.

>

*>Disabling the messenger service alone does not do very much to  
>increase the security of most home computers. There is currently only  
>one known vulnerability in the messenger service, and there is a patch  
>for that vulnerability. I would argue that leaving the messenger  
>service enabled with the patch installed can increase your security  
>compared to disabling the service.*

Again, I would disagree. Months ago I argued that the Messenger Service was a risk if you didn't need it to run. I suggested that at any time a vulnerability could be discovered and exploited in it – just like sendmail. I was ridiculed about that notion. Now why in the world would we think that this would be the one and only vulnerability in this service? Oh, I know, we'll use Internet Explorer as an example. Only one vulnerability was ever found in it and Microsoft fixed it immediately and there's never been a problem with it since, right?

What should speak volumes in this particular case is the fact that Microsoft in its next service pack and subsequent OS releases is *\*disabling\** the Messenger Service just because of the reasons I mentioned. Bottom line is if you don't need the service, turn it off. If you need it or don't know if you do leave the default settings.

Suggesting that this service provides some beneficial unintended side effect as a warning system is quite a stretch, IMO. The only time it would act as such if someone sent a net send message to you. While not extremely rare, it doesn't happen to every one every day, let alone have it happen so frequently that it would warn you within minutes of your firewall being down. So in effect, by suggesting it is a valuable warning system when in fact it is a very lousy one, people can easily develop a false sense of security.

>

*>The goal of computer security is not to become 100% secure no matter  
>what the cost.*

You can never be 100% secure. And I never said that one could. But I am wondering, exactly what *\*cost\** is there in taking 30 seconds of one's life and disabling the Messenger Service?

---

What could possibly go wrong?