

## Re: [Full-Disclosure] Odd Behavior – Windows Messenger Service

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-07/0616.html>

---

*From:* Neil McKellar (*mckellar\_at\_telusplanet.net*)

*Date:* 07/18/03

To: full-disclosure@lists.netsys.com  
Date: Thu, 17 Jul 2003 23:39:22 -0600

Please be patient with me while I work through this a bit. I want to be sure I understand.

In morning\_wood's original post, he said:

- > *Windows® networking ( TCP) and messenger service are both initialized*
- > *before any user/admin login has taken place, and are remotely*
- > *accessible*

He went on to describe getting some Messenger spam before he's even logged in. It's true that Messenger is a dog. And in another message, morning\_wood says:

- > *my post is in regard of Windows Messenger being accessible without*
- > *any interactive login to take place*

Given what Messenger typically gets used for, I don't think that's a bad question.

But then we get this, and morning\_wood isn't the only one suggesting this:

- > *imho it is irresponsible default behavior for a workstation OS to*
- > *allow remote resources / services / enumeration before any*
- > *interactive user or administrative login.*

So suppose. You're on a local network with a central authentication service of some kind. Maybe it's a Windows domain controller, maybe it's NIS+, maybe it's Kerberos. Whatever.

Now, we've decided to follow your advice and *\*not\** enable any remote resources/services/enumeration before login. Just to be clear, is there a TCP stack yet or is this a 'resource' or 'service'? How do I actually *\*do\** the login against the remote authentication service without activating some kind of service before the login?

I'm also curious about what exactly we mean by 'workstation'? If 'workstation' is a stand-alone computer and necessary peripherals (ie. hard drive, monitor, etc.), then maybe for some value of "no services"

Full-Disclosure: Re: [Full-Disclosure] Odd Behavior – Windows Messenger Service

we can successfully get the user logged in.

If we also include diskless workstations or thin-clients that boot off the network or terminal clients (X-terminals/Windows Terminal Server), this becomes much harder. These machines \*need\* to be running services and network connected just to get booted up and display a login prompt.

I'm asking because I want to be clear about what morning\_wood and others are suggesting should be the default. If I've misunderstood, please explain yourselves. I'm just going on what I see here.

If we're actually nitpicking about \*which\* services should be running, then I think you're preaching to the choir here. :-) Yes, a lot of stuff gets turned on by default that \*nobody\* needs and certainly not on a workstation. True of a lot of Linuxes, Unixes, and Windows boxes.

--  
Neil (mckellar@telusplanet.net)

---

Full-Disclosure - We believe in it.  
Charter: <http://lists.netsys.com/full-disclosure-charter.html>