

RE: Using Messenger Service for 'Net Send' Functionality ---- Dangerous? Why?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-06/0034.html>

From: Meni Milstein (meni_at_kdm.co.il)

Date: 06/11/05

Date: Sat, 11 Jun 2005 18:34:43 +0300
To: 'Matt Ostiguy' <ostiguy@gmail.com>

As far as I can remember the only problem with the messenger was the fact that you kept receiving pop-up ads from the internet. That's why everyone started disabling it.

MS articles: <http://support.microsoft.com/default.aspx?scid=kb;en-us;330904>

In my networks (without specific relevance to messenger service) I close the NetBIOS and UDP broadcast traffic (as stated in the above article). Closing these services to the WWW will ensure you won't get the annoying popups, and that no one from the outside will be able to contact your messenger service enabled users.

Good luck.

Meni Milstein.

<http://www.lcs-guides.com>

-----Original Message-----

From: Matt Ostiguy [<mailto:ostiguy@gmail.com>]
Sent: Saturday, June 11, 2005 12:03 AM
To: focus-ms@securityfocus.com
Subject: Re: Using Messenger Service for 'Net Send' Functionality ---- Dangerous? Why?

Ugh. There isn't much of an audit trail for it (as opposed to email notifications, for example). There is no security on it whatsoever--any nitwit could

net send * bad message here

resulting in everyone on the subnet getting a "bad message here" popup

You'd be reliant upon a working WINS infrastructure, but would still have issues if the specific user was not logged in. If a user is logged into > 1 machine, I believe only the last machine they logged

SecurityFocus Microsoft: RE: Using Messenger Service for 'Net Send' Functionality ---- Dangerous? Why?

into will get it (as my WINS console only shows my username registered once for the [03h] netbios name type.

So, you would be potentially activating another service, thus gaining whatever potential security vulnerabilities lie within, only to obtain a fairly unreliable notification method.

Matt

On 2 Jun 2005 19:20:04 -0000, deadly.halo@gmail.com

<deadly.halo@gmail.com> wrote:

> *A fellow network administrator at the company I work for is interested in implementing a system that utilizes the Messenger Service (not to be confused with the MS Messenger chat tool) to initiate Net Send notifications to clients throughout the user community. Our network hosts consist of Windows 2000/XP machines (XP has the service disabled by default, 2000 may as well). I remember that there was a large vulnerability reported at the end of 200*