

SecurityFocus Bugtraq: Re: Microsoft got it wrong

Re: Microsoft got it wrong

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-10/0185.html>

From: T.A. Adjuster (adjuster_at_peeved.org)

Date: 10/16/03

To: "Richard M. Smith" <rms@computerbytesman.com>, "'Giovanni Campagnoli'" <bioia@yahoo.com>, <bu
Date: Thu, 16 Oct 2003 12:59:29 -0400

The article (<http://support.microsoft.com/?kbid=828035>) referred to in Mr. Campagnoli's original posting refers not to the "Windows Messenger", but to the "Messenger" service, traditionally used to display messages of the "NET SEND" or "WinPopup" variety.

The "Messenger" service runs, at least in Windows 2000, as "Local System", and is set to "Automatic" startup in all versions of Windows NT back to, I believe, 3.51.

In the context of a buffer-overflow in the "Messenger" service being undiscovered, the USA Today article echoes the sentiment that I would express: "Messenger" service pop-ups are a nuisance and nothing more.

In the context of the buffer-overflow as described in the Microsoft article above, and assuming that the overflow is exploitable, I would consider this a critical security concern.

Assuming that, at the time of the USA Today article's writing, the overflow was undiscovered, I would argue that Microsoft did not "get it wrong".

As a matter of course, I have been disabling the "Messenger" service in new installations for the past several years and would recommend that everyone do so (using Active Directory Group Policies to disable services is a beautiful thing). The frustrating part of this, however, is the usage of this mechanism by some software to "broadcast" messages to clients (UPS management software comes to mind first). Perhaps this represents an opportunity for someone to implement a better "Messenger listener" that could gateway these messages to other protocols or logs.

As an aside, this also highlights a frustration that I've had with Microsoft on several occasions-- naming products or components of products similar names. I've seen confusion between the "Messenger" service and "Windows Messenger", the "Computer Browser" service and web browsers, and long ago confusion between the "Microsoft Exchange" MAPI client software and "Microsoft Exchange Server".

T.A. Adjuster

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

From: "Richard M. Smith" <rms@computerbytesman.com>

Re: Microsoft got it wrong

SecurityFocus Bugtraq: Re: Microsoft got it wrong

To: "'Giovanni Campagnoli'" <bioia@yahoo.com>; <bugtraq@securityfocus.com>

Sent: Wednesday, October 15, 2003 4:51 PM

Subject: Microsoft got it wrong

Only last month in USA Today, Microsoft was claiming that Windows Messenger didn't represent a security hazard:

Pop-ups assail through Windows

http://www.usatoday.com/tech/news/2003-09-24-popups_x.htm

Microsoft views pop-up boxes as a benign nuisance that does "not pose a security risk," says Greg Sullivan, product manager for Windows.

Looks like Microsoft crystal ball is pretty fuzzy. Windows Messenger is just the sort of seldom-used feature that should be turned off by default in Windows XP.

Richard M. Smith

<http://www.ComputerBytesMan.com>