

## RE: MSN Messenger reveals your name to websites (and can reveal email addresses too)

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-02/0083.html>

---

*From:* Bryan Allerdice ([bryan\\_allerdice@yahoo.com](mailto:bryan_allerdice@yahoo.com))

*Date:* 02/06/02

From: "Bryan Allerdice" <[bryan\\_allerdice@yahoo.com](mailto:bryan_allerdice@yahoo.com)>

To: <[vuln-dev@securityfocus.com](mailto:vuln-dev@securityfocus.com)>

Date: Tue, 5 Feb 2002 22:19:39 -0400

An email was posted to a security mailing list today or yesterday by Johannes Westerink concerning Cross Site Scripting on Microsoft domains...

<snip>

Examples how it can be exploited:

Cross Site Scripting:

~~~~~

[http://ulogin.bcentral.com/~>alert\(document.cookie\)</script>.aspx?aspxerrorpath=null](http://ulogin.bcentral.com/~>alert(document.cookie)</script>.aspx?aspxerrorpath=null)

[http://www.msn.com/~>alert\(document.cookie\)</script>.aspx?aspxerrorpath=null](http://www.msn.com/~>alert(document.cookie)</script>.aspx?aspxerrorpath=null)

[http://my.msn.com/~>alert\(document.cookie\)</script>.aspx?aspxerrorpath=null](http://my.msn.com/~>alert(document.cookie)</script>.aspx?aspxerrorpath=null)

[http://dotnet.microsoft.com/>alert\(document.cookie\)</script>.aspx](http://dotnet.microsoft.com/>alert(document.cookie)</script>.aspx)

[http://terraserver.microsoft.net/>alert\(document.cookie\)</script>.aspx](http://terraserver.microsoft.net/>alert(document.cookie)</script>.aspx)

x

[http://support.microsoft.com/~>alert\(document.cookie\)</script>.aspx?aspxerrorpath=null](http://support.microsoft.com/~>alert(document.cookie)</script>.aspx?aspxerrorpath=null)

[http://office.microsoft.com/~>alert\(document.cookie\)</script>.aspx?aspxerrorpath=null](http://office.microsoft.com/~>alert(document.cookie)</script>.aspx?aspxerrorpath=null)

[http://communities.microsoft.com/~>alert\(document.cookie\)</script>.aspx](http://communities.microsoft.com/~>alert(document.cookie)</script>.aspx)

[http://uddi.microsoft.com/~>alert\(document.cookie\)</script>.aspx](http://uddi.microsoft.com/~>alert(document.cookie)</script>.aspx)

<snip>

Since Microsoft domains are trusted, and get email address details using Richard's code, couldn't a CSS version be made which grabs full user details, and relays them to an untrusted third party?

I'm busy working at the moment, but I am interested if it can be done. How about someone out there with more time on their hands than me, give the CSS idea a go and report back to the list.

I'm sure spammers will love this exploit... unfortunately. Thanks Microsoft.

Poor XP users.

BRYAN

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

From: Richard Burton [mailto:[richardaburton@hotmail.com](mailto:richardaburton@hotmail.com)]

Sent: Saturday, February 02, 2002 4:39 PM

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

Subject: MSN Messenger reveals your name to websites (and can reveal email addresses too)

Introduction

=====

MSN Messenger (and Windows Messenger on XP) can be used to obtain personal information about a user from any website (in any domain).

Using JavaScript a user's display name can be obtained from Messenger, as well as the display names of all their contacts. For users who have a sensible and accurate display name this should be considered a privacy issue. (Note: anyone who has not set a display name at all, will reveal their email address instead.)

Using the same technique web sites hosted on certain domains (microsoft.com, hotmail.com & hotmail.msn.com) can also access the email address of the user (along with the email addresses of all their contacts). This could be used by Microsoft to track users on their sites, which many would consider to be a privacy issue.

In addition to the three domains mentioned above, additional domains can be allowed access to the email addresses with a single registry entry. This registry entry could be made by spyware/adware installed by a user (sometimes unknowingly along with a piece of shareware). Once there you have the potential to give your email address to any site that requests it and places it in a cookie.

Affects

=====

- MSN Messenger 4.6.0073 (latest at 02/02/2002) on Windows 2000 with IE 6.

- Windows Messenger 4.6.0073 (latest at

02/02/2002) on Windows XP with IE 6.

– Probably other versions and other platforms too.

#### Technical

=====

Microsoft designed Messenger to allow functionality to be used in webpages using JavaScript or VBScript. This includes the ability to view the display name and email address of the user and their contacts. In an attempt to protect users only a certain selection of sites can use script to get email addresses, but all can get display names.

The list of domain suffixes that have full access to Messenger functionality (email addresses & more?) can be found in the registry in key "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MessengerService\Policies\Suffixes".

Values "Suffix0", "Suffix1", etc. By default there are no entries in the list, but they can be added. E.g. adding value Suffix0 = "test.com" will give web sites in the test.com domain full access to Messenger information.

Full domains do not have to be specified in the list, adding "com" would allow all .com sites to have full access.

Although by default there are no entries in this list, three domains (listed above) are hard coded into Messenger for the same purpose. These allow Microsoft to make their sites (e.g. Hotmail) look nice by integrating messenger features into them. The user cannot remove the special status applied to these sites.

The only way for a user to prevent sites having any access to their information is by logging out of Messenger before visiting.

For a simple how-to, just look at the source of the demonstration page given below.

#### Demo Page

=====

I have set up a simple demonstration of the problem here:

<http://raburton.members.easyspace.com/msn/>

This will show your name and the names of all your contacts. If you add the registry entry given it will also show your email address and the addresses of all your contacts.

#### Recommendations For Users

=====

- Set a display name so your email address isn't obtainable so easily.
- Check for entries in "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MessengerService\Policies\Suffixes" regularly, especially after installing freeware or shareware.
- If you want to visit microsoft.com and remain anonymous, close MSN Messenger.

#### Recommendations For Microsoft

=====

- Remove the hard coded list of domains, so users can choose to allow this functionality on MS sites.
- Prevent applications adding to the Suffixes list.
- Give the user the option to disable the scripting support.

#### Author

=====

Richard Antony Burton - [richardaburton@hotmail.com](mailto:richardaburton@hotmail.com)

Please feel free to contact me about this post, I will do my best to answer any questions you may have.

---

Do You Yahoo!?

Get your free @yahoo.com address at <http://mail.yahoo.com>

---

Do You Yahoo!?

Get your free @yahoo.com address at <http://mail.yahoo.com>

- 
- **Previous message:** [Sean Davis: "Re: chaging your @home IP address... could you take a bunch of them....probably... could you get something from it...maybe"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)