

# MSN messenger improper file transfer ip-address field parsing

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-11/0256.html>

---

**From:** ronan o kane (*hi\_t3ch\_ass4ssin\_at\_hotmail.com*)

**Date:** 11/21/03

Date: 21 Nov 2003 02:38:27 -0000

To: bugtraq@securityfocus.com

('binary' encoding is not supported, stored as-is)

MSN Messenger bug

Release Date:

20/11/03

Discovery date:

Sometime around 2001 or 2000

Versions Affected:

-----

Msn messenger 1.0 -> msn messenger 6.0.0602

Windows messenger all versions

Not Affected:

-----

Msn Messenger 6.1, trillian, gaim

Description:

-----

A bug exists in Microsofts msn messenger client. MSN messenger improperly parses the fields during file transfer invitation requests. Particularly the request ip field. This makes it possible to trick the msn client into giving *\*away\** the users ip address without him/her accepting the file transfer first.

The bug happens when a specially crafted MSG requests are issued to the switchboard server and then relayed onto the client. Upon receiving each

## SecurityFocus Bugtraq: MSN messenger improper file transfer ip-address field parsing

request from the switchboard the client seems to incorrectly process the Ip-Address field without first waiting for userB to accept the file that is being attempted to be sent. It seems the reason for this bug is that the msn client seems to unsafely depend on client of userB to send the sequences and fields in those sequences in the order in which is expected. A malicious user however could construct a program that sends them in the incorrect order and requests userB for the ip address before userB asks userA for its ip address and userBs client will falsely hand out the ip address. This circumvents the whole thing and allows us to invade the users privacy by handing out such sensitive info.

Below are example of \*expected\* exchange of data (this however can be exploited)

Example:

>>> MSG 4 N 277

MIME-Version: 1.0

Content-Type: text/x-msmsgsinvite; charset=UTF-8

Application-Name: File Transfer

Application-GUID: {5D3E02AB-6190-11d3-BBBB-00C04F795683}

Invitation-Command: INVITE

Invitation-Cookie: 33267

Application-File: readme.txt

Application-FileSize: 60904

<<< MSG example@passport.com Tim 179

MIME-Version: 1.0

Content-Type: text/x-msmsgsinvite; charset=UTF-8

Invitation