

Buffer overflow in MSN Messenger 6.0

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-07/0246.html>

From: Bahaa Naamneh (b_naamneh_at_hotmail.com)

Date: 07/19/03

Date: 19 Jul 2003 11:42:26 -0000

To: bugtraq@securityfocus.com

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

#####

Application: MSN Messenger 6.0

<http://www.msnmessenger-download.com/Preview/>

Affected Versions: MSN Messenger 6.0 build 6.0.0501 and prior

Bug: Buffer overflow in msnmsgr.exe

(In the small viewer box that show the sending file before accepting it).

Author: Bahaa Naamneh

e-mail: b_naamneh@hotmail.com

#####

=====

Introduction:

=====

MSN Messenger is one of the most famous messengers, due to the interesting services that it offer.

the version 6.0 appear with many services, one of this services is the small viewer box that show the icon of the sending file before getting it,if the sending file is picture this box show the picture itself not the icon before getting it. picture of the viewer box

(<http://members.lycos.co.uk/bnsecurity/msn/msn01.JPG>)

=====

The bug (buffer overflow):

=====

Sending "uncompleted pictures" cause a buffer overflow.

"Uncompleted pictures": I don't know if this phrase is correct, anyway I mean by this phrase the pictures that we didn't received it completely. Sometimes while we receiving picture from any person the connection failed or something happen that cause of nonbeing receiving the whole pictures

SecurityFocus Bugtraq: Buffer overflow in MSN Messenger 6.0

but although that we still can open it but it appear two parts the first part is the receiving part and the second part appear with dark color. picture of "Uncompleted pictures":

(<http://members.lycos.co.uk/bnsecurity/msn/msn03.JPG>).

You can download "uncompleted picture" from this link.

<http://members.lycos.co.uk/bnsecurity/01/>

(disable any downloading programs like getright or DAP ... if u use)

when u send "uncompleted picture" via messenger 6.0 the small viewer will lose the default size that it programmed to be.

<http://members.lycos.co.uk/bnsecurity/msn/msn03.JPG>

So sending the "uncompleted picture" will cause of Buffer overflow and Messenger will crash.

<http://members.lycos.co.uk/bnsecurity/msn/msn04.JPG>

=====

Vendor Response:

=====

Contacted. The bug have already fixed in build 6.0.0602

Microsoft Response: "...We suspect that we have already fixed this bug as early as build 501 as your report is very similar to a bug that was resolved with that build—but we would like your assistance to verify this. ..."

=====

Exploit:

=====

I'm trying to make an exploit in "visual basic"!!!.

You can download the "uncompleted picture" from this link:

<http://members.lycos.co.uk/bnsecurity/01/>

and test it by sending it via the messenger 6.0

#####

..Sorry for my poor english