

# [NT] Buffer Overflow in MSN Messenger

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0073.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 07/20/03

To: list@securiteam.com

Date: 20 Jul 2003 19:44:15 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----  
Buffer Overflow in MSN Messenger  
-----

## SUMMARY

MSN Messenger is "one of the most famous messengers, due to the interesting services that it offers". Version 6.0 comes with many new services and features, one of these is a small viewer box that displays a preview picture of the file being received before it actually starts receiving/sending it (Whenever the file being received is a picture). This preview has been found to contain a vulnerability whenever an incomplete picture is being received/sent.

## DETAILS

Vulnerable systems:

\* MSN Messenger version 6.0 build 6.0.0501

Immune systems:

\* MSN Messenger version 6.0 build 6.0.0602

An example incomplete picture can be downloaded from:

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

Securiteam: [NT] Buffer Overflow in MSN Messenger

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

Vendor 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, however, we would like your assistance to verify this."

ADDITIONAL INFORMATION

The information has been provided by <mailto:b\_naamneh@hotmail.com> Bahaa Naamneh.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.