

[NT] MSN Messenger OCX Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0049.html>

From: support@securiteam.com

Date: 05/09/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 9 May 2002 07:12:05 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

MSN Messenger OCX Buffer Overflow

SUMMARY

A vulnerability has been discovered in the parameter handling of the MSN Messenger OCX. By exploiting this vulnerability, an attacker can supply and execute code on any machine on which MSN Messenger with the ActiveX is installed.

The vulnerability exists because of how MSN Messenger handles data passed to it that can lead to a buffer overflow scenario. The buffer overflow can be exploited via email, web, or through any other method where Internet Explorer is used to display HTML that an attacker supplies, including software that uses the web browser ActiveX control.

All users of Internet Explorer are potentially affected because this is a Microsoft signed OCX. Users that have not installed Microsoft Messenger or that have not upgraded Microsoft Messenger can only be affected if they accept the pop-up "Install Now" signed by Microsoft. All Internet Explorer users should install the update.

DETAILS

Systems Affected:

- * Microsoft MSN Chat Control

- * Microsoft MSN Messenger 4.5 and 4.6, which includes the MSN Chat

Securiteam: [NT] MSN Messenger OCX Buffer Overflow

control

* Microsoft Exchange Instant Messenger 4.5 and 4.6, which includes the MSN Chat control

Example:

```
<Object classid="clsid:9088E688-063A-4806-A3DB-6522712FC061" width="455"
height="523">
<param name="_cx" value="12039">
<param name="_cy" value="13838">
<param name="BackColor" value="50331647">
<param name="ForeColor" value="43594547">
<param name="RedirectURL" value="">
<param name="ResDLL" value="AAAAAAA[27,257 bytes is where the EIP
starts]">
</object>
```

(We have replaced the letter O with 0 to prevent accidental execution)

Technical Description:

MSNChat OCX is an ActiveX object installed with Microsoft Messenger. Proper bounds checking are not in place in the ResDLL parameter. By supplying a very large buffer, we can overwrite a significant portion of the stack, including saved return addresses and exception handlers.

Even if users do not have Messenger installed, the ActiveX can be called from the codebase tag which would prompt the user to install the ActiveX with Microsoft's credentials because the OCX is signed by Microsoft.

Vendor Status:

Microsoft has released a security bulletin and patch. For more information visit:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-022.asp>
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-022.asp>

ADDITIONAL INFORMATION

The information has been provided by <mailto:marc@eeye.com> Marc Maiffret.

=====

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

=====
=====

Securiteam: [NT] MSN Messenger OCX Buffer Overflow

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.

- ***Previous message:*** support@securiteam.com: "[NT] Unchecked Buffer in MSN Chat Control Can Lead to Code Execution"
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)