

ADVISORY: MSN Messenger OCX Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-05/0019.html>

From: Marc Maiffret (marc@EEYE.COM)

Date: 05/09/02

Date: Wed, 8 May 2002 16:00:05 -0700
From: Marc Maiffret <marc@EEYE.COM>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

MSN Messenger OCX Buffer Overflow

Release Date:

5/8/2002

Severity:

High (Remote code execution)

Systems Affected:

Microsoft MSN Chat Control

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

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

Chat control

Description:

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 which 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.

Example:

```
<object classid="clsid:9088E688-063A-4806-A3DB-6522712FC061" width="455" height="523">
```

NT-Bugtraq: ADVISORY: MSN Messenger OCX Buffer Overflow

```
<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>
```

Technical Description:

MSNChat ocx is an ActiveX object installed with Microsoft Messenger. Proper bounds checking is 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.

Vulnerability identifier: CAN-2002-0155

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>

Credit:

Discovery: Drew Copley

Greetings: Mom, Dad, and all of the little people that helped me and believed in me – oh – and a big YO HO to the homeboyz in the h00d.

Copyright (c) 1998-2002 eEye Digital Security

Permission is hereby granted for the redistribution of this alert electronically. It is not to be edited in any way without express consent of eEye. If you wish to reprint the whole or any part of this alert in any other medium excluding electronic medium, please e-mail alert@eEye.com for permission.

Disclaimer

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

Feedback

Please send suggestions, updates, and comments to:

NT-Bugtraq: ADVISORY: MSN Messenger OCX Buffer Overflow

eEye Digital Security
<http://www.eEye.com>
info@eEye.com

- *Previous message:* [Ry Jones: "NTFS and PGP interact to expose EFS encrypted data"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)