CERT Advisory CA-2002-13 Buffer Overflow in Microsoft's MSN Chat ActiveX Control

Original release date: May 10, 2002
Last revised: August 28, 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Microsoft Windows systems with one or more of the following:

- Microsoft MSN Chat control
- Microsoft MSN Messenger 4.6 and prior
- Microsoft Exchange Instant Messenger 4.6 and prior

Overview

Microsoft's MSN Chat is an ActiveX control for Microsoft Messenger, an instant messaging client. A buffer overflow exists in the ActiveX control that may permit a remote attacker to execute arbitrary code on the system with the privileges of the current user.

I. Description

A buffer overflow exists in the "ResDLL" parameter of the MSN Chat ActiveX control that may permit a remote attacker to execute arbitrary code on the system with the privileges of the current user. This vulnerability affects MSN Messenger and Exchange Instant Messenger users. Since the control is signed by Microsoft, users of Microsoft's Internet Explorer (IE) who accept and install Microsoft-signed ActiveX controls are also affected. The Microsoft MSN Chat control is also available for direct download from the web.

The <object> tag could be used to embed the ActiveX control in a web page. If an attacker can trick the user into visiting a malicious site or the attacker sends the victim a web page as an HTML-formatted email message or newsgroup posting then this vulnerability could be exploited. This acceptance and installation of the control can occur automatically within IE for users who trust Microsoft-signed ActiveX controls. When the web page is rendered, either by opening the page or viewing the page through a preview pane, the ActiveX control could be invoked. Likewise, if the ActiveX control is embedded in a Microsoft Office (Word, Excel, etc.) document, it may be executed when the document is opened.

According to the Microsoft Advisory (MS02-022):

> *It's important to note that this control is used for chat rooms on several MSN sites in addition to the main MSN Chat site. If you have successfully used chat on any MSN-site, you have downloaded and installed the chat control.*

The CERT/CC has published information on ActiveX in *Results of the Security in ActiveX Workshop* (pdf) and CA-2000-07.

This issue is also being referenced as CAN-2002-0155:

> *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0155*

II. Impact

A remote attacker may be able to execute arbitrary code with the privileges of the current user.

III. Solution

Apply a patch from your vendor

On June 11, 2002, Microsoft updated Microsoft Advisory (MS02-022) and released a new patch that remedies the vulnerability for users that downloaded and accepted the control. The previous solution did not fully protect against this action and it was possible for an attacker to load the vulnerable control, even though the previous patch and updated versions had been installed.

The new patch is available at http://www.microsoft.com/Downloads/Release.asp?ReleaseID=39632. All users should apply this patch, even if you previously installed an updated version of your software. This patch supercedes the patch information below.

> *Microsoft has released a patch, a fixed MSN Chat control, and upgrades to address this issue. It is important that all users apply the patch since it will prevent the installation of the vulnerable control on systems that have not already installed it.*
>
> *Download location for the patch:*
>
> > *http://www.microsoft.com/Downloads/Release.asp?ReleaseID=38790*

If you have updated your software prior to June 11, 2002, you should reinstall the software from the following locations:

> *Download location for updated version of MSN Messenger with the corrected control:*
>
> > *http://messenger.msn.com/download/download.asp?client=1&update=1*
>
> *Download location for updated version of Exchange Instant Messenger with the corrected control:*
>
> > *http://www.microsoft.com/Exchange/downloads/2000/IMclient.asp*

Microsoft also suggests that the following Microsoft mail products: Outlook 98 and Outlook 2000 with the Outlook Email Security Update, Outlook 2002, and Outlook Express will block the exploitation of this vulnerability via email because these products will open HTML email in the Restricted Sites zone.

Other mitigation strategies include opening web pages and email messages in the Restricted Sites zone and using email clients that permit users to view messages in plain-text. Likewise, it is important for users to realize that a signed control only authenticates the origin of the control and does not imply any information with regard to the security of the control. Therefore, downloading and installing signed controls through an automated process is not a secure choice.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, please check the Vulnerability Note (VU#713779) or contact your vendor directly.

Microsoft

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

The CERT/CC acknowledges the eEye Team for discovering and reporting on this vulnerability and thanks Microsoft for their technical assistance.

Feedback can be directed to the author: Jason A. Rafail

Revision History

```
May 10, 2002:  Initial release
August 28, 2002:  Updated patch information
```