

# [NT] Unchecked Buffer in MSN Chat Control Can Lead to Code Execution

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0048.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 05/09/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Thu, 9 May 2002 07:06:58 +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.

-----

Unchecked Buffer in MSN Chat Control Can Lead to Code Execution

---

## SUMMARY

The MSN Chat control is an ActiveX control that allows groups of users to gather in a single, virtual location online to engage in text messaging. The control is offered for download as a single ActiveX control from a number of MSN sites. In addition, it is included with MSN Messenger since version 4.5 and Exchange Instant Messenger. While the MSN Chat control is included with these products it is not used to provide Instant Messaging functionality, but rather to add chat functionality to those products.

An unchecked buffer exists in one of the functions that handle input parameters in the MSN Chat control. A security vulnerability results because it is possible for a malicious user to levy a buffer overrun attack and attempt to exploit this flaw. A successful attack could allow code to run in the user's context.

It would be possible for an attacker to attempt to exploit this vulnerability either through a malicious web site or through HTML email. However, Outlook Express 6.0 and the Outlook Email Security Update, which is available for Outlook 98 and Outlook 2000, Outlook 2002 and can thwart such attempts through their default security settings.

## Securiteam: [NT] Unchecked Buffer in MSN Chat Control Can Lead to Code Execution

### DETAILS

#### Affected Software:

- \* 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

#### Mitigating factors:

- \* A successful attack would require that the user have installed the MSN Chat control, MSN Messenger, or Exchange Instant Messenger.
- \* The MSN Chat control does not install with any version of Windows or Internet Explorer by default.
- \* Windows Messenger which ships with Windows XP does not include the MSN Chat control. Windows XP users would be vulnerable only if they have chosen to install the MSN Chat control from MSN sites.
- \* The HTML email attack vector is blocked by the following Microsoft mail products: Outlook 98 and Outlook 2000 with the Outlook Email Security Update, Outlook 2002, and Outlook Express. This is because these products all open HTML email in the Restricted Sites zone by default.

#### Patch availability:

##### Download locations for the patch:

- \* Download locations for the patch:  
<<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=38790>>  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=38790>

##### Download Locations for Updated Software Versions:

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

#### What is the scope of the vulnerability?

This is a buffer overflow vulnerability. An attacker who successfully exploited this vulnerability would be able to run programs on another user's system. Such a program could take any action that the system's owner could take, such as adding, changing, or deleting any data or configuration information. For example, the code could lower the security settings in the browser, or write a file to the hard disk.

The affected component does not ship by default with any version of Windows or IE. Customers who are using the latest Microsoft mail products, Outlook 2002 and Outlook Express 6.0 are protected by default against HTML

## Securiteam: [NT] Unchecked Buffer in MSN Chat Control Can Lead to Code Execution

email-borne attacks. Outlook 98 and Outlook 2000 customers who have applied the Outlook Email Security Update are also protected by default against HTML email-borne attacks. Because the code would run as the user and not the operating system, any security limitations on the user's account would also be applicable to any code run by successfully exploiting this vulnerability. In environments where user accounts are restricted, such as enterprise environments, the actions that an attacker's code could take would be limited by these restrictions.

What causes the vulnerability?

The vulnerability results because of an unchecked buffer in the code that handles the input of a parameter in the MSN Chat control. By invoking this parameter in a particular manner, an attacker could overflow the buffer and gain the ability to run code in the user's security context.

What is MSN Chat?

MSN Chat is an online service offered by MSN that lets users talk to one another in virtual "chat rooms". These rooms can allow multiple users to gather in a single, virtual location and exchange text-based messages.

MSN Chat works by users running a local client chat program, in this case the MSN Chat control, and then logging on to a central chat server. Once logged on to the chat server, users can enter chat rooms and exchange messages with one another.

What is the MSN Chat control?

The MSN Chat control is an ActiveX control that is used on a variety of MSN sites, including the MSN Chat site. In essence, the control is a self-contained chat program

What is an ActiveX control?

ActiveX is a technology that allows developers to deploy programs in a small, self-contained way. These programs are called controls and can be used by web pages, Visual Basic programs or other applications.

ActiveX controls can be distributed in a number of ways including installing with software products or being offered for download from a web site. Regardless of how a user installs an ActiveX control, once it is installed and registered on the user's system, it is fully functional and available to the user.

How do I get the MSN Chat control?

You can get the MSN Chat control through two means:

- \* Via web download from MSN Chat sites.
- \* Through inclusion with Microsoft Instant Messaging Products, specifically MSN Messenger and Exchange Instant Messenger.

How do I get the MSN Chat control from the web?

Any time a user visits a chat room on MSN, the site checks to see if the user's system has the latest version of the MSN Chat control. If no control is found on the user's system or a newer version of the control is

## Securiteam: [NT] Unchecked Buffer in MSN Chat Control Can Lead to Code Execution

available than is on the user's system, the MSN Chat control is automatically offered for download. The user then has the choice to accept and install the control, or cancel the download. If the user chooses to accept the control, it is then installed.

It is 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.

How do I get the MSN Chat control from Microsoft Instant Messaging Products?

In addition to being available for download directly from the MSN Chat site, the MSN Chat control is installed with MSN Messenger, since version 4.5, and Exchange Instant Messenger.

It is important to note however, that this vulnerability does not affect these technologies themselves. MSN Chat is different from MSN Messenger, Windows Messenger, or Exchange Instant Messenger in that those technologies are peer-to-peer messaging products and allow users to talk directly with each other. While users of these technologies logon to a directory server, to announce their availability, there are no "rooms" as in MSN Chat, and users exchange messages directly with one another.

The vulnerability in question only affects the MSN Chat control and not MSN Messenger or Exchange Instant Messenger.

Is the MSN Chat control included with Windows Messenger in Windows XP?

No. The MSN Chat control is not included with Windows Messenger in Windows XP. However, Windows XP users can install the control by visiting an MSN Chat site and downloading the control.

What is wrong with the MSN Chat control?

An unchecked buffer in one of the functions that handles the input of certain parameters to the control.

What would this vulnerability enable an attacker to do?

An attacker who exploited this vulnerability successfully could run a program on a system that had the control installed. Since the MSN Chat control runs in the security context of the user, the program would be able to take any actions that the legitimate user was capable of taking, including adding or deleting data or configuration information.

On the other hand, this also means that any limitations placed on the user's account would apply to the attacker's code as well. For example, if an enterprise administrator had implemented policies such that the user could not change their IE security setting, the attacker's code would also be prevented from changing those settings.

How might an attacker attempt to exploit this vulnerability?

An attacker could attempt to exploit this vulnerability by creating a web

## Securiteam: [NT] Unchecked Buffer in MSN Chat Control Can Lead to Code Execution

page that invoked the MSN Chat control and included a call to the parameter in question in a particular way. When the user opened the web page and the code on the page ran, the attack would be carried out.

The attacker would most likely attempt to get the user to open this malicious web page in one of two ways:

- \* By posting the page on a web site. If he successfully enticed the user to visit his site, the control would be invoked once the page had loaded.
- \* By sending the web page as an HTML email to the user. When the web page was rendered, either by opening the mail or through a preview pane, the control would be invoked.

How can I mitigate the risk of the web-borne attack?

For the web-based attack to succeed, the attacker would have to lure the user to a site under his control. Users who exercise caution in their choice of web sites and only visited trusted web sites could potentially protect themselves from attack by avoiding the attacker's web site.

In addition, users who use the "Restricted Sites" zone when visiting untrusted sites can also mitigate their risk from this vulnerability. This is because, as discussed in Q174360, the Restricted Sites zone disables scripting of ActiveX control, rendering attempts to exploit this vulnerability ineffective.

I've heard that if I'm using IE, it's possible for an attacker to exploit this vulnerability even if I've never installed the MSN Chat control or the Messenger products, is that true?

It is true that it is possible for an attacker to host a copy of the vulnerable version of the control on their web site that could be offered for download when a user visited the site. However, the attacker would have to entice the user to visit their web site and convince the user to accept and install the control when offered.

Since the chat control is meant to be used in conjunction with chat sites, it would be worth questioning the trustworthiness of any site that unexpectedly offered a chat control for download. The best action would be to refuse the download offered.

But, I've heard that it's possible for an attacker to force this control to download without my knowing it, is that true?

Not exactly. There is an option that can allow a user to always accept signed code, such as the MSN Chat control, without prompting. Specifically, a user can select the "Always trust content from" check box that is presented when a signed control is offered for download.

However, the option only grants trust to the particular certificate that was used to sign that control, it does not grant blanket trust to the company or organization as a whole. This means that even if you have chosen to trust content signed by Microsoft, it does not necessarily mean that the particular certificate used to sign this control.

## Securiteam: [NT] Unchecked Buffer in MSN Chat Control Can Lead to Code Execution

Certificates are used to sign only a handful of controls. This means that only someone who has downloaded the chat control or other related controls from MSN and selected the "Always trust content from" option would have chosen to always trust content signed by this certificate.

Even then, the control could not be offered for download unless a user chooses to navigate to a site under an attacker's control. There is no way for an attacker to offer this control without a user visiting their site.

That said, the "killbit" will be set for this vulnerable control in an upcoming IE service pack, to ensure that this unusual scenario does not pose a risk for customers.

What is the "killbit"?

There is a security feature in Internet Explorer that makes it possible to prevent an ActiveX control from ever being loaded by the system. This is accomplished by a making a registry setting and is referred to as setting the "killbit". Once the "killbit" is set, the control can never be loaded, even when it is fully installed. Setting this ensures that even if a vulnerable component is introduced or re-introduced onto a system it remains inert and harmless.

There is more information on this feature in <http://www.microsoft.com/technet/support/kb.asp?ID=240797> Q240797.

How can I mitigate the risk of the email-borne attack?

Customers who use any of the following products are protected against email-borne attacks by default:

- \* Outlook 98 and Outlook 2000 if the Outlook Email Security Update has been installed.
- \* Outlook 2002
- \* Outlook Express 6

This is because these products read email in the "Restricted Sites" zones. By default, the Restricted Sites zone disables the scripting of ActiveX control. This means that an HTML email that attempts to exploit the vulnerability that is read using one of these products is rendered harmless.

I am using one of the mail products listed above and do not visit untrustworthy sites. Does this mean I do not need the patch? While those products and habits can help protect you from attack without the patch, users should still upgrade their version of MSN Chat, MSN Messenger, or Exchange Instant Messenger or apply the patch to fully protect themselves.

How can I eliminate the vulnerability?

There are three recommended ways that users can eliminate the vulnerability.

## Securiteam: [NT] Unchecked Buffer in MSN Chat Control Can Lead to Code Execution

- \* Users can download an updated version of the MSN Chat control from the MSN Chat sites.
- \* Users can install an updated version of MSN Messenger
- \* Users can install an updated version of Exchange Instant Messenger

In addition, users can download and apply the patch as an immediate, interim measure to eliminate the vulnerability by unregistering the vulnerable control and setting the "killbit". However, it is recommended that users apply this patch only as an interim solution until they can install the appropriate updated software.

How do I install an updated version of the MSN Chat control from the MSN Chat sites?

Users who want to eliminate the vulnerability by downloading and installing an updated version of the MSN Chat control can go to the MSN Chat site, chat.msn.com and enter a chat room. The updated MSN Chat control will then be presented for download automatically and users can follow the instructions provided there to install the updated component.

What does the updated version of the MSN Chat control do?

The updated version of the MSN Chat control eliminates the vulnerability by implementing proper checking in the affected buffer. In addition, it automatically unregisters all previous versions of the MSN Chat control and sets the "killbit" to render them unusable.

How do I install an updated version of MSN Messenger?

Users who are running MSN Messenger and want to eliminate the vulnerability by installing the latest version of MSN Messenger can follow the instructions provided by MSN Messenger's AutoUpdate feature, or download the latest version from the location specified in the "Patch Availability" section.

What does the updated version of MSN Messenger do?

The updated version of MSN Messenger installs the updated MSN Chat control, which eliminates the vulnerability by implementing proper checks on the parameter input buffer. In addition, the updated MSN Chat control included in the updated version of MSN Messenger unregisters all previous versions of the MSN Chat control and sets the "killbit" to render them unusable.

How do I install an updated version of Exchange Instant Messenger?

Administrators who want to eliminate the vulnerability by installing an updated version of Exchange Instant Messenger in their environments can download the updated version from the location specified in the "Patch Availability" section.

What does the updated version of Exchange Instant Messenger do?

You can get the MSN Chat control through two means:

- \* Via web download from MSN Chat sites.
- \* Through inclusion with Microsoft Instant Messaging Products, specifically MSN Messenger and Exchange Instant Messenger.

## Securiteam: [NT] Unchecked Buffer in MSN Chat Control Can Lead to Code Execution

How do I install the patch?

Users can install the patch by downloading the patch from the location specified in the "Patch Availability" section.

What does the patch do?

The patch eliminates the vulnerability by unregistering the vulnerable MSN Chat control and sets the "killbit", rendering it useless.

Does the patch install an updated version of the MSN Chat control?

No. However, the next time a user visits the MSN Chat site after applying the patch, the updated version of the MSN Chat control will be offered for download.

### ADDITIONAL INFORMATION

The information has been provided by

<[mailto:0\\_30622\\_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C\\_US@Newsletters.Microsoft.com](mailto:0_30622_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com)>  
Microsoft Product Security.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[REVS] CRLF Injection"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)