

# [NT] Vulnerability in Microsoft's HTML Converter Could Allow Code Execution

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0046.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 07/14/03

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

Date: 14 Jul 2003 12:00:28 +0200

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

-----  
Vulnerability in Microsoft's HTML Converter Could Allow Code Execution  
-----

## SUMMARY

All versions of Microsoft Windows contain support for file conversion within the operating system. This functionality allows users of Microsoft Windows to convert file formats from one to another. In particular, Microsoft Windows contains support for HTML conversion within the operating system. This functionality allows users to view, import, or save files as HTML.

There is a flaw in the way the HTML converter for Microsoft Windows handles a conversion request during a cut-and-paste operation. This flaw causes a security vulnerability to exist. A specially crafted request to the HTML converter could cause the converter to fail in such a way that it could execute code in the context of the currently logged-in user. Because Internet Explorer uses this functionality, an attacker could construct a specially formed Web page or HTML e-mail that would cause the HTML converter to run arbitrary code on a user's system. A user visiting an attacker's Web site could allow the attacker to exploit the vulnerability

## Securiteam: [NT] Vulnerability in Microsoft's HTML Converter Could Allow Code Execution

without any other user action.

To exploit this vulnerability, the attacker would have to create a specially formed HTML e-mail and send it to the user. Alternatively, an attacker would have to host a malicious Web site that contains a Web page designed to exploit this vulnerability. The attacker would then have to persuade a user to visit that site.

### DETAILS

#### Vulnerable systems:

- \* Microsoft Windows 98
- \* Microsoft Windows 98 Second Edition
- \* Microsoft Windows Me
- \* Microsoft Windows NT 4.0 Server
- \* Microsoft Windows NT 4.0 Terminal Server Edition
- \* Microsoft Windows 2000
- \* Microsoft Windows XP
- \* Microsoft Windows Server 2003

#### Mitigating factors:

\* By default, Internet Explorer on Windows Server 2003 runs in Enhanced Security Configuration. This default configuration of Internet Explorer blocks automatic exploitation of this attack. If Internet Explorer Enhanced Security Configuration has been disabled, the protections put in place that prevent this vulnerability from being automatically exploited would be removed.

\* In the Web-based attack scenario, the attacker would have to host a Web site that contained a Web page used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site outside the HTML e-mail vector. Instead, the attacker would need to lure them there, typically by getting them to click a link that would take them to the attacker's site.

\* Exploiting the vulnerability would allow the attacker only the same privileges as the user. Users whose accounts are configured to have few privileges on the system would be at less risk than ones who operate with administrative privileges.

#### Patch Details:

Patch information and download can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS03-03.asp>>  
<http://www.microsoft.com/technet/security/bulletin/MS03-023.asp>

#### What's the scope of the vulnerability?

This is a buffer-overflow vulnerability. If an attacker were to successfully exploit this vulnerability – for example, if the user visits a site under the attacker's control or receives an HTML email from the attacker, then the HTML converter could allow arbitrary code to execute in the context of the logged on user.

## Securiteam: [NT] Vulnerability in Microsoft's HTML Converter Could Allow Code Execution

What causes the vulnerability?

The vulnerability results because of an unchecked buffer in the HTML converter that can be encountered when a cut-and-paste operation is made by a Web page to Internet Explorer.

What is an HTML converter?

The HTML converter is an extension that allows applications to convert HTML data into Rich Text Format (RTF) while maintaining the formatting and structure of the data as well as the text. The converter also supports the conversion of RTF data into HTML.

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker to cause Internet Explorer to fail in such a way that it could execute code of the attacker's choice.

This could allow an attacker to take any action on a user's system in the security context of the currently logged in user.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability by hosting a specially constructed Web page. If the user visited this Web page, Internet Explorer could fail and could allow arbitrary code to execute in the context of the user. Alternatively, an attacker could also craft an HTML email that attempted to exploit this vulnerability.

Does this mean the flaw is in Internet Explorer?

No – The flaw is in the underlying HTML conversion component in Windows. Internet Explorer has the ability to use this functionality and therefore exposes the vulnerability.

I am running Internet Explorer on Windows Server 2003. Does this mitigate this vulnerability?

Yes. By default, Internet Explorer on Windows Server 2003 runs in a restricted mode known as Enhanced Security Configuration.

What is Internet Explorer Enhanced Security Configuration?

Internet Explorer Enhanced Security Configuration is a group of preconfigured Internet Explorer settings that reduce the likelihood of a user or administrator downloading and running malicious Web content on a server. Internet Explorer Enhanced Security Configuration reduces this risk by modifying numerous security-related settings, including Security and Advanced tab settings in Internet Options. Some of the key modifications include:

- \* Security level for the Internet zone is set to High. This setting disables scripts, ActiveX Controls, Microsoft virtual machine (Microsoft VM), HTML content, and file downloads.

- \* Automatic detection of intranet sites is disabled. This setting assigns all intranet Web sites and all Universal Naming Convention (UNC) paths that are not explicitly listed in the Local intranet zone to the Internet zone.

## Securiteam: [NT] Vulnerability in Microsoft's HTML Converter Could Allow Code Execution

\* Install On Demand and non-Microsoft browser extensions are disabled. This setting prevents Web pages from automatically installing components and prevents non-Microsoft extensions from running.

\* Multimedia content is disabled. This setting prevents music, animations, and video clips from running.

Disabling Internet Explorer Enhanced Security Configuration would remove the protections put in place that help prevent this vulnerability from being exploited. For more information regarding Internet Explorer Enhanced Security Configuration, please consult the Managing Internet Explorer Enhanced Security Configuration guide, which can be found at the following location:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=d41b036c-e2e1-4960-99bb-9757f7e9e31b&DisplayL>  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=d41b036c-e2e1-4960-99bb-9757f7e9e31b&DisplayL>

Is there any configuration of Windows Server 2003 that is likely to have Internet Explorer Enhanced Security Configuration Disabled?

Yes. Systems Administrators who have deployed Windows Server 2003 as a Terminal Server would likely disable Internet Explorer Enhanced Security Configuration to allow users of the Terminal Server to use Internet Explorer in an unrestricted mode.

I'm running Outlook with the Outlook Email Security Update, Outlook 2002 or Outlook Express 6 SP1 in it's default configuration. Does this protect me from this vulnerability?

The default settings of Outlook 2002, Outlook Express 6.0 SP1, and Outlook 98 or Outlook 2000 with the Outlook Email Security Update installed do block the most obvious vector of attack through HTML email.

However, many other components of the Windows operating system can utilize the HTML Converter. Like the Outlook 2002 plain text workaround mentioned in the Workaround section, this is not a complete mitigating factor for this vulnerability.

What does the patch do?

The patch corrects the vulnerability by removing the unchecked buffer in the HTML converter.

Workarounds:

Are there any workarounds that can be used to block exploitation of this vulnerability while I am testing or evaluating the patch?

Yes. Although Microsoft urges all customers to apply the patch at the earliest possible opportunity, there are a number of workarounds that can be applied to help prevent the vector used to exploit this vulnerability in the interim.

It should be noted that these workarounds should be considered temporary measures as they just help block paths of attack rather than correcting the underlying vulnerability.

## Securiteam: [NT] Vulnerability in Microsoft's HTML Converter Could Allow Code Execution

The following sections are intended to provide you with information to help protect your computer from attack. Each section describes the workarounds that you may want to use depending on your computer's configuration.

### \* Rename HTML32.cnv

Renaming the HTML32.CNV file will help prevent the vulnerability from being exploited. To rename this file, perform the following steps:

1. Click on the Start button
2. Click on the menu item Run
3. Type explorer to open Windows Explorer
4. Click on the Search button in the upper toolbar
5. Search for the file HTML32.cnv
6. Right-click on the file name HTML32.cnv in the search window
7. Click on Rename in the menu items
8. Change the last 3 characters in the filename from "cnv" to "old"

### \* Disable Allow paste operations via script in the Internet zone:

You can help protect against this vulnerability by changing your settings for the Internet security zone to disable "Allow paste operations via script". To do this, perform the following steps:

1. In Internet Explorer, select Tools, Internet Options
2. Click on the Security tab
3. Highlight the Internet icon and click on the Custom Level button
4. Scroll through the list to the Scripting section
5. Under Allow paste operations via script click Disable
6. Click OK, then click OK again to return to Internet Explorer

### \* Turn off active scripting support in Internet Explorer

You can turn off support for active scripting by performing the steps in the following knowledge base article:

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:154036>>  
<http://support.microsoft.com/default.aspx?scid=kb:en-us:154036>

Note that disabling scripting support in Internet Explorer will affect the functionality of many Web sites on the Internet and should be considered a temporary workaround only.

### \* Restrict Web sites to only your trusted Web sites

As another workaround for this vulnerability, you can add sites that you trust to the Trusted sites zone in Internet Explorer after disabling active scripting in the Internet zone. This will allow you to continue using trusted Web sites exactly as you do today, while tightening the restrictions on un-trusted sites. When you are able to deploy the patch, you will be able to re-enable active scripting in the Internet zone.

To do this, perform the following steps:

- \* Select Tools, then Internet Options. Click the Security tab.

## Securiteam: [NT] Vulnerability in Microsoft's HTML Converter Could Allow Code Execution

\* In the box labeled Select a Web content zone to specify its current security settings, click Trusted Sites, then click Sites

\* If you want to add sites that do not require an encrypted channel, click to clear the Require server verification (https:) for all sites in this zone check box.

\* In the box labeled Add this Web Site to the zone, type the URL of a site that you trust, then click the Add button. Repeat for each site that you want to add to the zone.

\* Click OK twice to accept the changes and return to Internet Explorer.

Add any sites that you trust not to take malicious action on your computer. One in particular that you may want to add is <http://windowsupdate.microsoft.com>. This is the site that hosts the patch, and it requires active scripting to install the patch.

Note that there is generally a trade-off between ease-of-use and security; by selecting a high-security configuration, you could make it extremely unlikely that a malicious Web site could take action against you, but at the cost of missing a lot of rich functionality. The appropriate balance between security and ease-of-use is different for everyone, and you should pick a configuration that fits your needs. The good news is that it's easy to change your configuration, and you can try different configurations until you find the right one for you until you can install the patch.

\* If you are using Outlook 2002, to help protect yourself from the HTML email attack vector, read email in plain text format. Users of Microsoft Outlook 2002 who have applied Service Pack 1 can enable a feature to view all non-digitally-signed e-mail or non-encrypted e-mail messages in plain text only.

Digitally signed e-mail or encrypted e-mail messages are not affected by the setting and may be read in their original formats. Information on enabling this setting in Outlook 2002 can be found in the following Knowledge Base article:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:307594>  
<http://support.microsoft.com/default.aspx?scid=kb:en-us:307594>

<Are there any side effects to renaming HTML32.CNV?> Are there any side effects to renaming HTML32.CNV?

Yes. When performing certain actions in Microsoft FrontPage, you might receive the following error:

```
Unable to run text converter c:\Program Files\Common Files\Microsoft Shared\Textconv\Html32.cnv
```

\* If you insert a file in FrontPage and choose any Office file format, it will fail with this error.

## Securiteam: [NT] Vulnerability in Microsoft's HTML Converter Could Allow Code Execution

\* If you drag an Office file to an open .htm page in FrontPage, it will fail with this error.

If you require this functionality, you should consider enacting one of the other supplied workarounds.

Are there any side-effects to disabling active scripting?

Yes. Many Web sites on the Internet use scripting to provide additional functionality. For instance, an online e-commerce site or banking site might use active scripting to provide menus, ordering forms, or even account statements.

Disabling active scripting is a global setting for all Internet sites. If you feel that there are sites on the Internet where you require the page to use active scripting, you can instead use the "Restrict Web sites to only your trusted Web sites" workaround.

Are there any side-effects to disabling paste operations from scripts in the Internet zone?

Yes. Paste operations will not work correctly from script in Internet Explorer for sites viewed in the Internet zone.

Are there any side effects to restricting Web sites from my trusted Web sites?

Yes. For those sites you have not configured to be in your Trusted sites zone, their functionality will be impaired if they require active scripting to display properly. Adding sites to your Trusted sites zone will cause them to be able to use active scripting and display correctly. However, you should only add Web sites you trust to the Trusted sites zone.

Are there any side-effects to reading email in plain text format?

Yes. E-mail viewed in plain text format cannot contain pictures, specialized fonts, animations, or other rich content. In addition:

- \* The changes are applied to the preview pane and open messages.
- \* Pictures become attachments to avoid loss.
- \* The object model (custom code solutions) may behave unexpectedly because the message is still in Rich Text or HTML format in the mail store.

### ADDITIONAL INFORMATION

Original advisory can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS03-023.asp>>  
<http://www.microsoft.com/technet/security/ulletin/MS03-023.asp>

=====

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:

Securiteam: [NT] Vulnerability in Microsoft's HTML Converter Could Allow Code Execution

[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.