

# More CERT Information

Most of this information is very “geekily” written. It might be hard to understand. Sorry about that!

## Vulnerability Note VU#205148

### Microsoft Internet Explorer does not properly evaluate Content-Type and Content-Disposition headers

#### Overview

A cross-domain scripting vulnerability exists in the way Microsoft Internet Explorer (IE) evaluates Content-Type and Content-Disposition headers and checks for files in the local browser cache. This vulnerability could allow a remote attacker to execute arbitrary script in a different domain, including the [Local Machine Zone](#).

#### I. Description

Microsoft Security Bulletin [MS03-032](#) describes a vulnerability in the way IE checks for files in the local browser cache:

*A flaw in Internet Explorer could allow a malicious Web site operator to access information in another Internet domain, or on the user's local system by injecting specially crafted code when the browser checks for the existence of files in the browser cache. ...There is a flaw in the way Internet Explorer checks the originating domain when checking for the existence of local files in the browser cache.*

SNS Advisory [No.67](#) further elaborates:

*If specific MIME type is specified in the Content-Type header of an HTTP response and if a special string is defined in the Content-Disposition header, this string can be automatically downloaded and opened within the Temporary Internet Files (TIF) under several conditions in Microsoft Internet Explorer. ...Additionally, if this vulnerability is exploited through a specific string in the Content-Disposition header, the OBJECT tag can be parsed in the "My Computer" zone.*

Presumably, specially crafted Content-Type and Content-Disposition headers can cause IE to execute script in a different domain, including the Local Machine Zone. It seems that the contents of the Content-Disposition header is treated as HTML code, and any

script in those contents is executed without regard to cross-domain security restrictions. For some reason, IE considers the script to be in the Local Machine Zone, when files in the Temporary Internet Files directory should not be trusted and are typically treated as if they were in the Internet zone.

## II. Impact

An attacker who is able to convince a user to access a specially crafted HTML document, such as an Internet web page or HTML email message, could execute arbitrary script with privileges of the user in the security context of the Local Machine Zone. This technique could be used to read certain types of files in known locations on the user's system. In conjunction with other vulnerabilities ([VU#626395](#), [VU#25249](#)), the attacker could execute arbitrary commands on the user's system. The attacker could also determine the path to the Temporary Internet Files folder (cache) and access data from other web sites.

## III. Solution

### Apply patch

Apply 822925 or a more recent cumulative patch for IE. See Microsoft Security Bulletin [MS03-032](#).

### Systems Affected

Vendor	Status	Date Updated
<a href="#">Microsoft Corporation</a>	Vulnerable	25-Aug-2003

### References

[http://www.lac.co.jp/security/english/snsadv\\_e/67\\_e.html](http://www.lac.co.jp/security/english/snsadv_e/67_e.html)  
[http://www.microsoft.com/security/security\\_bulletins/ms03-032.asp](http://www.microsoft.com/security/security_bulletins/ms03-032.asp)  
<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;822925>  
<http://msdn.microsoft.com/workshop/security/szone/overview/overview.asp>  
<http://www.secunia.com/advisories/9580/>  
<http://www.securityfocus.com/bid/8457>  
<http://xforce.iss.net/xforce/xfdb/12961>

### Credit

Microsoft credits LAC/SNS for reporting this vulnerability. Information used in this document came from LAC/SNS and Microsoft.

This document was written by Art Manion.

## Other Information

Date Public 08/20/2003

Date First Published 08/25/2003 03:55:37 PM

Date Last Updated 08/26/2003

CERT Advisory [CA-2003-22](#)

CVE Name [CAN-2003-0531](#)

Metric 20.27

Document Revision 22

If you have feedback, comments, or additional information about this vulnerability, please send us [email](#).

<http://www.kb.cert.org/vuls/id/205148>

# Vulnerability Note VU#548964

## Microsoft Windows BR549.DLL ActiveX control contains vulnerability

### Overview

The Microsoft Windows BR549.DLL ActiveX control, which provides support for the Windows Reporting Tool, contains an unknown vulnerability. The impact of this vulnerability is not known.

### I. Description

Microsoft Security Bulletin MS03-032 briefly describes a vulnerability in the BR549.DLL ActiveX control:

*This patch also sets the [Kill Bit](#) on the BR549.DLL ActiveX control. This control implemented support for the Windows Reporting Tool, which is no longer supported by Internet Explorer. The control has been found to contain a security vulnerability. To protect customers who have this control installed, the patch prevents the control from running or from being reintroduced onto users' systems by setting the Kill Bit for this control.*

The vulnerability may be a buffer overflow. Presumably, the ActiveX control could be instantiated by Internet Explorer (IE) and the vulnerability could be exploited when a victim viewed a specially crafted HTML document such as a web page or HTML email message.

The class ID (CLSID) for this ActiveX control is 167701E3-FDCF-11D0-A48E-006097C549FF.

## II. Impact

The impact of this vulnerability is not known. In the case of a buffer overflow, a remote attacker could execute arbitrary code with the privileges of the user running IE. The attacker could also cause a denial of service.

## III. Solution

### Apply patch

Apply 822925 or a more recent cumulative patch for IE. See Microsoft Security Bulletin [MS03-032](#).

### Systems Affected

Vendor	Status	Date Updated
<a href="#">Microsoft Corporation</a>	Vulnerable	25-Aug-2003

### References

<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;822925>  
<http://support.microsoft.com/default.aspx?kbid=240797>  
<http://support.microsoft.com/default.aspx?kbid=154850>  
<http://www.secunia.com/advisories/9580/>  
<http://xforce.iss.net/xforce/xfdb/12962>  
<http://www.securityfocus.com/bid/8454>  
<http://securitytracker.com/alerts/2003/Aug/1007538.html>

### Credit

Microsoft credits Greg Jones of KPMG UK for reporting this vulnerability.

This document was written by Art Manion.

### Other Information

Date Public 08/20/2003

Date First Published 08/26/2003 01:40:23 AM

Date Last Updated 09/12/2003

CERT Advisory [CA-2003-22](#)

CVE Name [CAN-2003-0530](#)

Metric 7.78

Document Revision 16

If you have feedback, comments, or additional information about this vulnerability, please send us [email](#).

<http://www.kb.cert.org/vuls/id/548964>

## Vulnerability Note VU#865940

### Microsoft Internet Explorer does not properly evaluate "application/hta" MIME type referenced by DATA attribute of OBJECT element

#### Overview

Microsoft Internet Explorer (IE) will execute an HTML Application (HTA) referenced by the DATA attribute of an OBJECT element if the Content-Type header returned by the web server is set to "application/hta". An attacker could exploit this vulnerability to execute arbitrary code with the privileges of the user running IE.

**Note:** (2003-10-04) The patch provided by [MS03-040](#) addresses two attack vectors that were not resolved by [MS03-032](#).

#### I. Description

##### 1. The OBJECT element

The IE Dynamic HTML Object Model (DOM) defines the OBJECT element as a way to embed ActiveX controls and other objects in HTML documents. The DATA attribute is a URI that provides the data for an object, such as an HTML file (e.g., <OBJECT DATA="somefile.html">).

##### 2. The HTML Application (HTA)

HTML Applications (HTAs) are HTML documents that are executed as trusted

applications that are not subject to IE security restrictions. HTAs can run script, Java, or ActiveX controls. From Microsoft [documentation](#):

***Warning** HTAs can potentially expose the client machine to malicious script. HTAs, like .exe files have read/write access to the files and system registry on the client machine. Powerful executables can be produced and delivered quickly with a few short script statements. Use of HTAs is not recommended where security or the source of the file is questionable.*

### 3. IE MIME type determination

Instead of accepting the server-supplied Content-Type header as recommended in [RFC 2616](#), IE uses a rather [complicated method](#) to determine the MIME type of a file referenced by a URI. In many cases, IE will download and parse a file as part of the MIME type determination process. This check is unable to differentiate between HTA and HTML files since both files are essentially text files that contain HTML code. As a result, IE accepts the MIME Content-Type provided by the server.

### 4. The problem

When accessing an HTA file directly, IE prompts the user to download or run the file. However, when an HTA file is referenced by the DATA attribute of an OBJECT element, and the web server returns the Content-Type header set to "application/hta", IE may execute the HTA file directly, without user intervention. The HTML used to reference the HTA file can be created in at least three ways:

1. The HTML can be static
2. The HTML can be generated by script (<<http://lists.netsys.com/pipermail/full-disclosure/2003-September/009639.html>>)
3. The HTML can be generated by [Data Binding](#) an XML source to an HTML consumer (<<http://lists.netsys.com/pipermail/full-disclosure/2003-September/009665.html>>)

The extension of the HTA file does not affect this behavior, for example <OBJECT DATA="somefile.jpg"> (where somefile.jpg is a text file containing HTML code). IE security zone settings for ActiveX controls may prevent an HTA from being executed in this manner.

Any program that uses the WebBrowser ActiveX control or the IE HTML rendering engine (MSHTML) may be affected by this vulnerability. Outlook and Outlook Express are affected, however, recent versions of these programs open mail in the Restricted Sites Zone where ActiveX controls and plug-ins and Active scripting are disabled by default.

This vulnerability is documented in an [advisory](#) from eEye Digital Security and Microsoft Security Bulletins [MS03-032](#) and [MS03-040](#).

The CERT/CC has received reports of this vulnerability being exploited to install backdoors and DDoS tools, read AIM credentials from the registry, install porn dialers, and modify DNS settings ([QHosts](#)). See Incident Note [IN-2003-04](#) for further information.

## II. Impact

By convincing a victim to view an HTML document (web page, HTML email), a remote attacker could execute arbitrary code with the privileges of the victim.

### **III. Solution**

#### **Apply patch**

Apply the patch (828750) referenced in Microsoft Security Bulletin [MS03-040](#) or a more recent cumulative patch. [CAN-2003-0838](#) and [CAN-2003-0809](#) correspond to the attack vectors that use script (2) and XML Data Binding (3), respectively.

The patch (822925) referenced in Microsoft Security Bulletin [MS03-032](#) (released on 2003-08-20) stops HTAs from executing in one case in which static HTML is used to create an OBJECT element referencing the HTA(1). The patch does not prevent HTAs from executing in at least two other cases in which the requisite HTML is generated by script (2) or by XML Data Binding (3).

#### **Disable ActiveX controls and plug-ins**

It appears that disabling the "Run ActiveX controls and plug-ins" setting will prevent OBJECT elements from being instantiated, thus preventing exploitation of this vulnerability. Disable "Run ActiveX controls and plug-ins" in the Internet Zone and any zone used to read HTML email. In our tests, this setting prevented OBJECT elements from being instantiated and therefore stopped sample exploits from running. It has been [reported](#) that disabling ActiveX controls and plug-ins is not completely effective.

#### **Apply the Outlook Email Security Update**

Another way to effectively disable ActiveX controls and plug-ins in Outlook is to install the Outlook Email Security Update. The update configures Outlook to open email messages in the Restricted Sites Zone, where ActiveX controls and plug-ins and Active scripting are disabled by default. In addition, the update provides further protection against malicious code that attempts to propagate via Outlook. The Outlook Email Security Update is available for [Outlook 98](#) and [Outlook 2000](#). The functionality of the Outlook Email Security Update is included in Outlook 2002 and Outlook Express 6.

#### **Unmap HTA MIME type**

Deleting or renaming the following registry key prevents HTAs from executing in the three cases listed above:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\MIME\Database\Content  
Type\application/hta
```

Note that there may be other attack vectors that do not rely on this MIME setting.

#### **Block Content-Type headers**

Use an application layer firewall, HTTP proxy, or similar technology to block or modify HTTP Content-Type headers with the value "application/hta". This technique may not work for encrypted HTTP connections and it may break applications that require the "application/hta" Content-Type header.

### **Block mshta.exe**

Use a host-based firewall to deny network access to the HTA host:

%SystemRoot%\system32\mshta.exe. Examining network traces of known attack vectors, it seems that the exploit HTML/HTA code is accessed three times, twice by IE and once by mshta.exe. The HTA is instantiated at some point before the third access attempt. Blocking mshta.exe prevents the third access attempt, which appears prevent the exploit code from being loaded into the HTA. There may be other attack vectors that circumvent this workaround. For example, a vulnerability that allowed data in the browser cache to be loaded into the HTA could remove the need for mshta.exe to access the network. This technique may break applications that require HTAs to access the network. Also, specific host-based firewalls may or may not properly block mshta.exe from accessing the network.

### **Maintain updated antivirus software**

Antivirus software with updated virus definitions may identify and prevent some exploit attempts. Variations of exploits or attack vectors may not be detected. Do not rely on antivirus software to defend against this vulnerability. The CERT/CC maintains a partial list of [antivirus vendors](#).

### **Systems Affected**

<b>Vendor</b>	<b>Status</b>	<b>Date Updated</b>
<a href="#">Microsoft Corporation</a>	Vulnerable	5-Oct-2003

### **References**

VU#626395

<http://www.eeye.com/html/Research/Advisories/AD20030820.html>

<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>

<http://support.microsoft.com/default.aspx?scid=kb;en-us;822925>

[http://msdn.microsoft.com/workshop/networking/moniker/overview/appendix\\_a.asp](http://msdn.microsoft.com/workshop/networking/moniker/overview/appendix_a.asp)

<http://msdn.microsoft.com/workshop/author/dhtml/reference/objects/object.asp>

<http://msdn.microsoft.com/workshop/author/hta/overview/htaoverview.asp>

<http://msdn.microsoft.com/workshop/author/hta/reference/objects/hta.asp>

[http://msdn.microsoft.com/workshop/author/om/doc\\_object.asp](http://msdn.microsoft.com/workshop/author/om/doc_object.asp)

[http://msdn.microsoft.com/workshop/author/databind/data\\_binding.asp](http://msdn.microsoft.com/workshop/author/databind/data_binding.asp)

<http://www.ietf.org/rfc/rfc2616.txt>

<http://www.secunia.com/advisories/9580/>  
<http://www.securityfocus.com/archive/1/334459>  
<http://xforce.iss.net/xforce/xfdb/12960>  
<http://lists.netsys.com/pipermail/full-disclosure/2003-September/009639.html>  
<http://lists.netsys.com/pipermail/full-disclosure/2003-September/009665.html>  
<http://lists.netsys.com/pipermail/full-disclosure/2003-September/009671.html>  
<http://greymagic.com/adv/gm001-ie/>  
<http://securityresponse.symantec.com/avcenter/venc/data/backdoor.coreflood.dr.html>  
<http://securityresponse1.symantec.com/sarc/sarc.nsf/html/backdoor.coreflood.html>  
<http://securityresponse.symantec.com/avcenter/venc/data/download.aduent.trojan.html>  
<http://www.symantec.com/avcenter/venc/data/trojan.qhosts.html>  
<http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0310&L=ntbugtraq&F=P&S=&P=2603>  
<http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0309&L=ntbugtraq&F=P&S=&P=784>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0838>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0809>  
<http://pivx.com/larholm/unpatched/>

## Credit

Microsoft credits [eEye Digital Security](#) for reporting this vulnerability. Information used in this document came from eEye, Microsoft, and http\_equiv.

This document was written by Art Manion.

## Other Information

Date Public 08/20/2003

Date First Published 08/25/2003 11:50:42 AM

Date Last Updated 07/08/2004

CERT Advisory [CA-2003-22](#)

CVE Name [CAN-2003-0532](#)

Metric 56.70

Document Revision 133

If you have feedback, comments, or additional information about this vulnerability, please send us [email](#).

<http://www.kb.cert.org/vuls/id/865940>

# Vulnerability Note VU#813208

# Microsoft Internet Explorer does not properly render input type tag

## Overview

Microsoft Internet Explorer (IE) does not properly render an input type tag, allowing a remote attacker to cause a denial of service.

## I. Description

Microsoft Security Bulletin MS03-032 briefly describes

*...a flaw in the way Internet Explorer renders Web pages that could cause the browser or Outlook Express to fail. Internet Explorer does not properly render an input type tag. A user visiting an attacker's Web site could allow the attacker to exploit the vulnerability by viewing the site. In addition, an attacker could craft a specially formed HTML based e-mail that could cause Outlook Express to fail when the e-mail was opened or previewed.*

This is the only information available about this vulnerability.

## II. Impact

By convincing a victim to view a specially crafted HTML document (web page, HTML email) , a remote attacker could cause a denial of service.

## III. Solution

### Apply patch

Apply 822925 or a more recent cumulative patch for IE. See Microsoft Security Bulletin [MS03-032](#).

### Systems Affected

Vendor	Status	Date Updated
<a href="#">Microsoft Corporation</a>	Vulnerable	26-Aug-2003

### References

<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>

### Credit

This vulnerability was reported by Microsoft.

This document was written by Art Manion.

## Other Information

Date Public 08/20/2003

Date First Published 08/26/2003 03:02:29 AM

Date Last Updated 09/03/2003

CERT Advisory [CA-2003-22](#)

CVE Name

Metric 3.65

Document Revision 12

If you have feedback, comments, or additional information about this vulnerability, please send us [email](#).

<http://www.kb.cert.org/vuls/id/813208>

# Vulnerability Note VU#334928

## Microsoft Internet Explorer contains buffer overflow in Type attribute of OBJECT element on double-byte character set systems

### Overview

Certain versions of Microsoft Internet Explorer (IE) that support double-byte character sets (DBCS) contain a buffer overflow vulnerability in the Type attribute of the OBJECT element. A remote attacker could execute arbitrary code with the privileges of the user running IE.

### I. Description

Microsoft Security Bulletin [MS03-032](#) and SNS Advisory [No.68](#) describe a buffer overflow vulnerability in the Type attribute of the [OBJECT](#) element. This vulnerability only affects double-byte character set versions of IE (e.g. Japanese) and may be related to [VU#679556/CAN-2003-0344/MS030-020](#).

### II. Impact

By convincing a victim to view an HTML document (web site, HTML email message), a remote attacker could execute arbitrary code with the privileges of the victim.

### III. Solution

#### Apply patch

Apply 822925 or a more recent cumulative patch for IE. See Microsoft Security Bulletin [MS03-032](#).

#### Systems Affected

Vendor	Status	Date Updated
<a href="#">Microsoft Corporation</a>	Vulnerable	25-Aug-2003

#### References

[http://www.lac.co.jp/security/english/snsadv\\_e/68\\_e.html](http://www.lac.co.jp/security/english/snsadv_e/68_e.html)  
<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>  
<http://msdn.microsoft.com/workshop/author/dhtml/reference/objects/object.asp>  
<http://xforce.iss.net/xforce/xfdb/12970>  
<http://www.securityfocus.com/bid/7806>

#### Credit

Microsoft credits LAC/SNS for reporting this vulnerability. Information used in this document came from LAC/SNS and Microsoft.

This document was written by Art Manion.

#### Other Information

Date Public 08/20/2003  
Date First Published 08/26/2003 12:49:49 AM  
Date Last Updated 08/26/2003  
CERT Advisory [CA-2003-22](#)  
CVE Name  
Metric 7.09  
Document Revision 14

If you have feedback, comments, or additional information about this vulnerability, please send us [email](#).

<http://www.kb.cert.org/vuls/id/334928>

# Vulnerability Note VU#25249

## HHControl Object (showHelp) may execute shortcuts embedded in help files

### Overview

The HHCtrl ActiveX control has a serious vulnerability that allows remote intruders to execute arbitrary code, if the intruder can cause a compiled help file (CHM) to be stored "locally." Microsoft has released a security bulletin and a patch for this vulnerability, but the patch does not address all circumstances under which the vulnerability can be exploited. This document discusses some of the additional ways in which this vulnerability can be exploited. Some common circumstances under which this vulnerability can be exploited are addressed by the Microsoft patch; others are not. Read this document carefully with your network configuration in mind to determine if you need to take any action. In recent discussions with the CERT/CC, Microsoft has indicated they do not plan to alter the patch.

### I. Description

The Microsoft Windows HTML help facility (part of Internet Explorer) is able to execute arbitrary programs through an embedded "shortcut" in a compiled HTML file. This allows the help system to start wizards and other programs as part of the help facility. Unfortunately, it also makes it unsafe for users to open help files obtained from untrusted sources.

An attacker who can construct a malicious help file and place it in a location accessible by the victim may be able to cause this help file to be loaded and the embedded shortcuts executed without interaction from the victim. A malicious web site author may cause a compiled HTML help file to be opened through the Active Scripting *showHelp* call in Internet Explorer. Help files may also be opened in other environments that support Active Scripting, such as email messages in Outlook.

The specific exploit described (and corrected) by Microsoft involves an attacker who makes the malicious help files available via a UNC share. The patch corrects this aspect of the problem by allowing help files to execute shortcuts only when "located on the user's local machine." More information about Microsoft's security bulletin and their patch is available from

<http://microsoft.com/technet/security/bulletin/ms00-037.asp>  
<http://microsoft.com/technet/security/bulletin/fq00-037.asp>

## Preconditions Required for Exploitation

Unfortunately, the Microsoft patch does not address several significant ways in which the vulnerability can be exploited. The vulnerability can be exploited in any situation where all of the following conditions are met:

1. The attacker must entice or compel a victim who has Active Scripting enabled to open an email message or visit a web page. Alternatively, the attacker could attempt to trick the victim into opening the compiled help file, such as by sending it as an attachment in an email message. Since it is not yet widely recognized that help files have the potential to be just as dangerous as an untrusted executable, this may not be difficult.
2. The attacker must be able to place a malicious help file in a location accessible to the user when the Active Script is executed. The attacker must also be able to predict or guess the path to this file. If the patch described in [Microsoft Security Bulletin MS00-037](#) has been applied, this file may not reside on a UNC share (\\hostname\path\file). That is, if the patch has not been installed, an intruder must be able to place a file anywhere that the victim can access it. If the patch has been installed, the intruder must be able to place a file anywhere that the victim can access it except on UNC shares.
3. The Active Script mentioned above must run in a security zone that allows ActiveX controls to run and allows the scripting of controls that are marked "safe for scripting." The default security settings for the Internet Zone and the My Computer zone allow these actions to occur without warning prompts.
4. The HHCtrl ActiveX control must be installed and be marked "safe for scripting" and "safe for initialization." This is the default configuration when Internet Explorer is installed.

Note that all of these conditions, some of which are default conditions, must be met in order for an attacker to exploit this vulnerability. Changing some of these conditions may involve trade-offs between functionality and security.

In recent discussions with the CERT/CC, Microsoft has not indicated any intention of changing the help system's behavior. Therefore, to be completely protected from exploitation of this vulnerability, users must eliminate one or more of the preconditions listed above.

It is reasonable for a user to expect that simply visiting a web page is a safe activity, so eliminating the first precondition is difficult. Disabling Active Scripting or the execution of ActiveX controls prevents the vulnerability from being exploited, but it also prevents the normal operation of these features and is likely to affect the appearance and functionality of web pages. Removing the "safe for initialization" or "safe for scripting" attributes of the HHCtrl causes warning dialogs to be generated in a number of circumstances where they may not be expected.

## How an Attacker May Create "Local" Files

Although you may believe it is difficult or impossible for an intruder to place a file in a predictable location that is accessible to you, in fact, several common practices allow intruders to do just this.

While preventing an attacker from downloading files on the local system without warning is a valuable security practice, it is not sufficient as the single line of defense against the **execution** of malicious code. The CERT/CC recommends adopting one of several more conservative solutions, including disabling ActiveX controls or Active Scripting. More information on these solutions are included in the [Solution](#) section of this document.

If a site relies solely on limiting the attacker's ability to make malicious code accessible to the victim, the following activities are not safe:

- Sharing files via a network filesystem such as AFS, DFS, NFS, Novell Netware, or Windows shares when users map these drives to local drive letters. When the drive letter is not predictable but the path to the file is, the attacker may be able to make multiple exploit attempts because failed calls to *showHelp* generate no error messages. Access control lists cannot be used to defend yourself against this problem because the ACL facility allows the intruder to give you access to malicious files they control without your consent.
- Sharing physical disk drives in environments such as academic labs, Internet cafes, or libraries, where an attacker may be able to store malicious files in a writable local directory.
- Using any of several products that automatically extract attachments from email messages and place them in predictable locations. A notable example of this is Eudora.
- Using chat clients such as IRC-II, ICQ, or AOL Instant Messenger in modes that allow unsolicited file transfers to be placed in a local directory.
- Hosting an anonymous FTP site, if the upload directory is accessible by local users.

Engaging in any of these activities renders a site vulnerable to the problem described in this document.

In addition, multiple cross domain security vulnerabilities ([VU#162097](#), [VU#244729](#), [VU#400577](#), [VU#462451](#), [VU#585123](#), [VU#598147](#), [VU#711843](#), [VU#728563](#), [VU#739376](#)) could allow untrusted script to execute in the [Local Machine Zone](#). Script in the Local Machine Zone can programmatically create an HHCtrl object and use the shortcut command to execute arbitrary local programs. Several other vulnerabilities provide the ability to download arbitrary files to the victim's system. These vulnerabilities allow attackers to meet the "local" CHM file precondition.

## II. Impact

By using the *showHelp* Active Scripting call in conjunction with shortcuts embedded in a malicious help file, attackers are able to execute programs and ActiveX controls of their

choice. Since exploitation of the vulnerability requires an attacker to place a compiled help file (CHM) in a location accessible to the victim, it is usually trivial to include a malicious executable as well. In this situation, the attacker can take any action that the victim can.

The essence of the problem is this:

**The ability for an intruder to make a file accessible to a victim running Internet Explorer is equivalent to the ability to execute arbitrary code on the victim's system if several common preconditions are met.**

It is important to note that a number of other vulnerabilities facilitate the process of making a malicious CHM file accessible to a victim. Accessing untrusted HTML documents (web sites, HTML-formatted email messages) with Active Scripting enabled can allow attackers to exploit this vulnerability.

### III. Solution

Update HTML Help.

Install an updated version of HTML Help ([811630](#)). As described in Microsoft Security Bulletin [MS03-015](#), the updated HHCtrl control disables the Shortcut command in a compiled help file that has been opened with the showHelp method:

- *Only supported protocols [http:, https:, [file:](#), ftp:, ms-its:, or mk:@MSITStore:] can be used with showHelp to open a web page or help (chm) file.*
- *The [shortcut](#) function supported by HTML Help will be disabled when the help file is opened with showHelp. This will not affect the shortcut functionality if the same CHM file is opened by the user manually by double-clicking on the help file, or by through an application on the local system using the HTMLHELP( ) API.*

Note that the patches referenced in MS03-004 and MS03-015 completely disable the showHelp method. After installing either one of these patches, Internet Explorer will not be able to open help files.

**Caveat:** The CERT/CC developed the following information based on our independent tests using primarily Internet Explorer 5 on Microsoft Windows NT 4.0 and Windows 2000. Your results will vary based on your particular configuration. For some sites, the patch provided by Microsoft is adequate. For others, particularly those sites using non-Microsoft networking products, the patch does not provide complete protection. You will need to understand your network's configuration prior to deciding which, if any, changes are appropriate.

Configure Outlook to read email in the Restricted Zone.

Because an email message may start Internet Explorer automatically if Active Scripting is

enabled, the CERT/CC encourages you to configure your Outlook email client to use the Restricted Zone, and to disable Active Scripting in this zone. This solution should be implemented in addition to one of the changes mentioned earlier.

The steps for configuring Outlook to use the Restricted Zone are:

1. Start Outlook as you normally would.
2. From the **Tools** menu select **Options....** The Options dialog box appears.
3. Select the **Security** tab. The Security Options panel appears.
4. In the **Secure content** section, change the pull-down menu from **Internet** to **Restricted Sites**.
5. Click **Apply** to save your changes.
6. Click **OK** to close the Options dialog box.

We recommend similar steps for any other mail clients that support Active Scripting and Security Zones (or similar facilities to prevent the unwanted execution of scripts).

Another way to effectively disable Active scripting in Outlook is to install the Outlook Email Security Update. The update configures Outlook to open email messages in the Restricted Sites Zone, where Active scripting is disabled by default. The Outlook Email Security Update is available for [Outlook 98](#) and [Outlook 2000](#). The functionality of the Outlook Email Security Update is included in Outlook 2002 and Outlook Express 6.

### Disable Active Scripting and/or ActiveX controls in the Internet Zone.

One way to prevent the exploitation of this vulnerability is to limit the functionality available to attackers through the security zone feature of Internet Explorer. The CERT/CC recommends this solution as a way to protect against the vulnerability while retaining as much functionality as possible in the help system.

A security zone is a set of security settings applied to a web page based on the site the web page originated from. By default, all sites are in the Internet Zone, and disabling functionality in this zone can protect you from attackers at all sites not associated with another zone.

You may also need to reduce the settings in the Local Intranet Zone, if you do not trust all web sites within your DNS domain. In fact, the risk of exploitation by an inside attacker may be greater, since the ability to create a file accessible by you may be easier within a local area network.

One or more of the following options must be changed in the appropriate zones to protect against the vulnerability:

#### The **Active Scripting** option

Disabling Active Scripting is perhaps the best solution since it prevents the vulnerability from being exploited and doesn't present the user with warning dialogs. Setting this option to "Prompt" is not recommended, because the warning dialog will incorrectly imply that the action is safe, when in fact it is not.

### The **Run ActiveX controls and plug-ins** option

Disabling the execution of ActiveX controls is an option that protects against this vulnerability, but it also prevents plug-ins from executing normally. Since plug-ins for common applications such as Adobe Acrobat are included in this same category, setting the option to "Disable" results in significantly reduced functionality. For similar reasons, setting this option to "Prompt" is not recommended, because it is not always clear what the safe response should be.

An excellent solution (but perhaps requiring more administrative effort) is to set this option to "Administrator approved". In this setting, only those ActiveX controls approved by the administrator (using the Internet Explorer Administration Kit) will be executed. If the administrator includes most controls but specifically excludes the HHCtrl control, there is an attractive balance between security and functionality. For more information regarding this option, see

<http://www.microsoft.com/Windows/ieak/en/support/faq/default.asp>

### The **Script ActiveX controls marked safe for scripting** option

Disabling the scripting of ActiveX controls marked "safe for scripting" protects against this vulnerability but limits the normal operation of many controls used over the Internet. Setting this option to "Prompt" generates a warning dialog that is not strongly enough worded to reflect the danger inherent in the HHCtrl control.

If all three of these options are set to "Enable", which is the default in the Internet Zone, this vulnerability may be exploited. Improving the security settings of any of these three options will at least cause a warning dialog to appear and may prevent the exploit entirely.

Steps for changing your security zone settings for Internet Explorer 5 on Windows NT 4.0 are:

1. Start Internet Explorer as you normally would.
2. From the Tools menu select Internet Options.... The Internet Options dialog box appears.
3. Select the Security tab. The Security Options panel appears.
4. Select the zone you wish to change. For most users, this is the Internet Zone, but depending on your circumstances, you may need to repeat these steps for the Local Intranet Zone as well.
5. Click the Custom Level button. The Security Settings panel appears.
6. Change one or more of the following settings based on the information provided earlier and your desired level of security.
  - a. Set Run ActiveX controls and plug-ins to administrator approved, disable, or prompt.
  - b. Set Script ActiveX controls marked safe for scripting to disable or prompt.
  - c. Set Active scripting to disable or prompt.
7. Click OK to accept these changes. A dialog box appears asking if you are sure you want to make these changes.

8. Click Yes.
9. Click Apply to save your changes.
10. Click OK to close the Internet Options dialog box.

Security zones can also be used to enable Active Scripting and ActiveX controls at specific sites where you wish to retain this functionality. To place a site in the Trusted Sites Zone using Internet Explorer 5.0 on Windows NT 4.0,

1. Start Internet Explorer as you normally would.
2. From the **Tools** menu select **Internet Options...** The Internet Options dialog box appears.
3. Select the **Security tab**. The Security Options panel appears.
4. Select the **Trusted Sites** Zone.
5. Click the **Sites...** button.
6. Enter the name of the trusted site in the **Add this Web Site to the zone:** text box.
7. Click the **Add** button.
8. If a dialog box appears saying "Sites added to this zone must use the https:// prefix. This prefix assures a secure connection":
  - a. Click OK.
  - b. Add https:// to the beginning of the site name, and try to add the site again.
  - c. Or uncheck the box at the bottom of the dialog box marked Require server verification (https:) for all sites in this zone. Making this change reduces the security of your system by not requiring certificate based authentication, relying instead on DNS based verification which could be misleading. The CERT/CC encourages you not to make this change unless you fully understand the implications. If you choose not to require certificate based verification, you may wish to reduce other security settings for the Trusted Sites Zone.

9. Click **OK** to save the new list of sites.
10. Click **Apply** to save your changes.
11. Click **OK** to close the Internet Options dialog box.

Steps for managing Security Zones in other versions of Windows and Internet Explorer are similar.

Disable or Restrict the Shortcut and WinHelp commands.

The patch from Security Bulletin [MS02-055](#) (Q323255), Internet Explorer 6 Service Pack 1, and Windows XP Service Pack 1 provide the ability to disable the Shortcut and WinHelp commands or restrict their operation to specified directories. See Microsoft Knowledge Base Article [810687](#) for details.

The "My Computer" Zone

In addition to the four zones that are ordinarily visible, there is a fifth zone called the "My Computer" zone which is not ordinarily visible. Files on the local system are in the "My Computer" zone. You can examine and modify the settings in the "My Computer" through the registry. For more information, see

<http://support.microsoft.com/support/kb/articles/Q182/5/69.ASP>

The "My Computer" zone may also be managed through the Internet Explorer Administration Kit (IEAK).

The CERT/CC does not recommend modifications to the "My Computer" zone unless you have unusual security requirements and a thorough understanding of the ramifications, including the potential for loss of functionality.

Note, however, that if there is a vulnerability or condition that allows an attacker to create a file locally (such as through Eudora, for example) then this file will be subject to the security settings of the "My Computer" zone.

Active Scripts on a web page or in a mail message will continue to be subject to the security settings of the zone where the web page or mail client resides. In this case, disabling Active Scripting in untrusted locations, including the Internet Zone, provides the best defense.

### Change the attributes of the HHCtrl ActiveX control.

Because the HHCtrl control is central to the exploitation of this vulnerability, removing either the "safe for scripting" or the "safe for initialization" attribute in the registry corrects the problem. Unfortunately, removing these attributes prevents some features of the help system from operating normally, even if the help file is opened through some other application.

Implementing this solution will allow other ActiveX controls to function, including those referenced in Internet web pages. If you are unable to implement one of the solutions mentioned earlier, or you are willing to sacrifice help system features for more complete ActiveX functionality, then you may wish to consider this solution. This solution will provide warning dialogs when users open help files -- both malicious and benign help files.

To mark the HHCtrl ActiveX control as **not** "safe for scripting", remove this registry key:

```
HKEY_CLASSES_ROOT\CLSID\ {ADB880A6-D8FF-11CF-9377-00AA003B7A11}\  
Implemented Categories\ {7DD95801-9882-11CF-9FA9-00AA006C42C4}
```

To mark the HHCtrl ActiveX control as **not** "safe for initialization", remove this registry key:

HKEY\_CLASSES\_ROOT\CLSID\ {ADB880A6-D8FF-11CF-9377-00AA003B7A11}\Implemented Categories\ {7DD95802-9882-11CF-9FA9-00AA006C42C4}

Spaces in the keys listed above were added to improve HTML formatting and are not in the actual registry keys.

Only one of the two changes need to be made in order to prevent the exploitation of this vulnerability. Either of these changes will result in additional warning dialogs when a user opens compiled help files with references to the HHCtrl control, even if the help file is part of legitimate locally installed software.

Avoid accessing filesystems writable by untrusted users.

Because of the difficulty in implementing this solution correctly, the CERT/CC does not recommend relying on this solution. You may want to consider this solution only if you can implement it easily or if you have no other viable choices.

Care should be taken with any mechanism that might allow an untrusted user to download or otherwise cause a file to be accessible to the victim. This includes, but is not limited to, network-based file sharing mechanisms (AFS, DFS, Netware, NFS, Windows shares) and mail delivery programs that automatically extract attachments.

Also, if you choose to implement this solution, you need to be especially vigilant in your monitoring of security resources for information about new vulnerabilities that allow attackers to download files to your system. The impact of these vulnerabilities will be greater than if you had selected one of the solutions recommended above.

## Systems Affected

Vendor	Status	Date Updated
<a href="#">Microsoft Corporation</a>	Vulnerable	25-Oct-2000

## References

<http://www.microsoft.com/technet/security/bulletin/ms00-037.asp>  
<http://www.microsoft.com/technet/security/bulletin/fq00-037.asp>  
<http://www.microsoft.com/technet/support/kb.asp?ID=259166>  
<http://msdn.microsoft.com/library/tools/htmlhelp/chm/hh1start.htm>  
<http://www.securityfocus.com/bid/1033>  
<http://www.microsoft.com/technet/security/bulletin/MS03-004.asp>  
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;810847>  
<http://support.microsoft.com/?kbid=811630>

[us/htmlhelp/html/vsconshortcutov.asp](http://msdn.microsoft.com/workshop/author/dhtml/reference/methods/showhelp.asp)  
<http://msdn.microsoft.com/workshop/author/dhtml/reference/methods/showhelp.asp>  
<http://support.microsoft.com/?kbid=810687>

## **Credit**

Thanks to Georgi Guninski, who originally discovered this vulnerability and who also provided input used in the development of this document.

Cory Cohen was the primary author of this document, with some text by Shawn Hernan. Updated by Art Manion.

## **Other Information**

Date Public 03/01/2000

Date First Published 10/25/2000 02:23:48 PM

Date Last Updated 04/12/2004

CERT Advisory [CA-2000-12](#)

CVE Name [CVE-2000-0201](#)

Metric 40.50

Document Revision 22

If you have feedback, comments, or additional information about this vulnerability, please send us [email](#).

<http://www.kb.cert.org/vuls/id/25249>