

# [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0056.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 01/12/05

To: list@securiteam.com

Date: 12 Jan 2005 11:55:04 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Vulnerability in HTML Help Allows Code Execution (MS05-001)

---

## SUMMARY

This update resolves a newly-discovered, publicly reported vulnerability. A vulnerability exists in the HTML Help ActiveX control in Windows that could allow information disclosure or remote code execution on an affected system.

If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system could be less impacted than users who operate with administrative privileges.

## DETAILS

Affected Software:

\* Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000

Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=BE1B11C0-EF09-4295-8FB2-0FF17BA65460>>

Download the update

## Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

\* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=43201B00-298D-4C0C-A26F-AAEDF163FEB7>>

Download the update

\* Microsoft Windows XP 64-Bit Edition Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1FC58C5F-3A97-4B89-96C3-AAEFFCE28535>>

Download the update

\* Microsoft Windows XP 64-Bit Edition Version 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3B3878C9-57FB-45A9-B5C2-234AD538D6CC>>

Download the update

\* Microsoft Windows Server 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=23E619FE-F6DB-4666-A247-339F55B059CC>>

Download the update

\* Microsoft Windows Server 2003 64-Bit Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3B3878C9-57FB-45A9-B5C2-234AD538D6CC>>

Download the update

\* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me) Review the FAQ section of this bulletin for details about these operating systems.

### Non-Affected Software:

\* Microsoft Windows NT Server 4.0 Service Pack 6a

\* Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

### Affected Components:

\* Internet Explorer 6.0 Service Pack 1 when installed on Microsoft Windows NT Server 4.0 Service Pack 6a or Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6 Download the update

### CVE Information:

HTML Help ActiveX control Cross Domain:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1043>>

CAN-2004-1043

A cross-domain vulnerability exists in HTML Help ActiveX control that could allow information disclosure or remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited that page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

### Frequently asked questions (FAQ) related to this security update:

Does this update contain any changes to functionality?

This security update prevents the creation of an instance of the HTML Help Active X control in HTML content that is served from outside the Local Machine zone. This change may prevent certain kinds of Web-based applications from functioning correctly. To resolve this issue, the user or administrator can selectively enable this ability on a site-by-site basis. Alternatively, they can enable this ability on the basis of the zone. Examples of zones include the Local intranet zone and the Trusted sites zone.

## Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

For more information on how to allow trusted HTML Help content to be displayed from sites outside of the Local Machine Zone see <http://support.microsoft.com/kb/892675> Microsoft Knowledge Base Article 892675.

Can I enable trusted HTML Help content outside the Local Machine zone?

Yes. You can enable HTML Help content outside the Local Machine zone. You can allow specific sites or security zones to render HTML Help content. To do this, create either or both of the following registry keys.

Warning When you do this, be very selective and allow only sites or security zones that you trust.

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system.

Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

To allow specific sites to render HTML Help content:

1. Click Start, click Run, type Regedit in the Open box, and then click OK.
  2. Locate and then click the following registry subkey:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x
- Note If this registry subkey does not exist, create it.
3. On the Edit menu, point to New, and then click Key.
  4. Type HHRestrictions, and then press ENTER.
  5. Right-click the HHRestrictions subkey, point to New, and then click String Value.
  6. Type UrlAllowList, and then press ENTER.
  7. Right-click the UrlAllowList value and then click Modify.
  8. Add URL prefixes as a semi-colon separated list into the Value Data field, and then press ENTER.

For example,

<http://www.wingtip toys.com/help/helpdocuments:http://myintranetapplication/help/helpfiles> (without the quotation marks).

Note The Value Data field of this registry value is by default blank.

To allow all sites in a specific zone to render HTML Help content:

1. Click Start, click Run, type Regedit in the Open box, and then click OK.
  2. Locate and then click the following registry subkey:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x
- Note If this registry subkey does not exist, create it.
3. On the Edit menu, point to New, and then click Key.
  4. Type HHRestrictions, and then press ENTER.
  5. Right-click the HHRestrictions subkey, point to New, and then click DWORD Value.
  6. Type MaxAllowedZone, and then press ENTER.
  7. Right-click the MaxAllowedZone value and then click Modify.
  8. Change the Value Data field to a number between 0 and 4, and then press ENTER.

How does the extended support for Windows 98, Windows 98 Second Edition, and Windows Millennium Edition affect the release of security updates for these operating systems?

Microsoft will only release security updates for critical security issues.

## Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

Non-critical security issues are not offered during this support period. For more information about the Microsoft Support Lifecycle policies for these operating systems, visit the following <http://go.microsoft.com/fwlink/?LinkId=33327> Web site.

Are Windows 98, Windows 98 Second Edition, or Windows Millennium Edition critically affected by the vulnerability that is addressed in this security bulletin?

Yes. Windows 98, Windows 98 Second Edition, and Windows Millennium Edition are critically affected by this vulnerability. A Critical security update for these platforms is available and is provided as part of this security bulletin and can be downloaded from the Windows Update Web site. For more information about severity ratings, visit the following Web site.

Note Updates for localized versions of Microsoft Windows 98 and Microsoft Windows 98 Second Edition that are not supported by Windows Update Slovenian, Slovakian, and Thai are available for download at the following download location.

I am still using Microsoft Windows NT 4.0 Workstation Service Pack 6a or Windows 2000 Service Pack 2, but extended security update support ended on June 30, 2004. What should I do?

Windows NT 4.0 Workstation Service Pack 6a and Windows 2000 Service Pack 2 have reached the end of their life cycles, as previously documented.

Microsoft extended this support to June 30, 2004.

It should be a priority for customers who have these operating system versions to migrate to supported versions to prevent potential exposure to vulnerabilities. For more information about the Windows Product Lifecycle, visit the following Microsoft Support Lifecycle Web site. For more information about the extended security update support period for these operating system versions, visit the following Microsoft Product Support Services Web site.

Customers who require additional support for Windows NT Workstation 4.0 SP6a must contact their Microsoft account team representative, their technical account manager, or the appropriate Microsoft partner representative for custom support options. Customers who do not have an Alliance, Premier, or Authorized Contract can contact their local Microsoft sales office. For contact information, visit the Microsoft Worldwide Information Web site, select the country, and then click Go to see a list of telephone numbers. When you call, ask to speak with the local Premier Support sales manager.

For more information, see the Windows Operating System Product Support Lifecycle FAQ.

I am still using Windows XP, but extended security update support ended on September 30th, 2004.

The original version of Windows XP, commonly known as Windows XP Gold or Windows XP Release to Manufacturing (RTM) version, reached the end of its extended security update support life cycle on September 30, 2004.

It should be a priority for customers who have this operating system version to migrate to supported operating system versions to prevent potential exposure to vulnerabilities. For more information about the

## Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

Windows Service Pack Product Lifecycle, visit the Microsoft Support Lifecycle Web site. For more information about the Windows Product Lifecycle, visit the Microsoft Support Lifecycle Web site.

For more information, see the Windows Operating System Product Support Lifecycle FAQ.

I am still using Windows NT 4.0 Server, but extended security update support ended on December 31st, 2004. However, this bulletin has a security update for this operating system version. Why is that?

Windows NT 4.0 Server Service Pack 6a and Windows NT 4.0 Server Terminal Server Edition Service Pack 6 reached the end of their life cycles, as previously documented. However, the end-of-life occurred very recently. In this case, most of the steps that are required to address this vulnerability were completed before this date. Therefore, we have decided to release a security update for this operating system version as part of this security bulletin.

We do not anticipate doing this for future vulnerabilities that may affect this operating system version, but we reserve the right to produce updates and to make these updates available when necessary. It should be a priority for customers who have this operating system version to migrate to supported operating system versions to prevent potential exposure to vulnerabilities. For more information about the Windows Service Pack Product Lifecycle, visit the Microsoft Support Lifecycle Web site. For more information about the Windows Product Lifecycle, visit the Microsoft Support Lifecycle Web site.

For more information, see the Windows Operating System Product Support Lifecycle FAQ.

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 that is known as Enhanced Security Configuration. This mode mitigates this issue.

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 of an administrator downloading and running malicious Web content on a server. Internet Explorer Enhanced Security Configuration reduces this risk by modifying many security-related settings, including the settings on the Security and the Advanced tab in the Internet Options dialog box. Some of the important modifications include the following:

- \* Security level for the Internet zone is set to High. This setting disables scripts, ActiveX controls, Microsoft Java Virtual Machine (MSJVM), 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.

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

## Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

and prevents non-Microsoft extensions from running.

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

I am running Internet Explorer on Windows XP Service Pack 2. Does this mitigate this vulnerability?

No. While Internet Explorer on Windows XP Service Pack 2 does include changes to how HTML content is rendered in the Local Machine zone, this issue is not mitigated by these changes.

Can I use the Microsoft Baseline Security Analyzer (MBSA) to determine if this update is required?

Yes. MBSA will determine if this update is required. For more information about MBSA, visit the MBSA Web site.

Note After April 20, 2004, the Mssecure.xml file that is used by MBSA 1.1.1 and earlier versions is no longer being updated with new security bulletin data. Therefore, scans that are performed after that date with MBSA 1.1.1 or earlier will be incomplete. All users should upgrade to MBSA 1.2.1 because it provides more accurate security update detection and supports additional products. Users can download MBSA 1.2.1 from the MBSA Web site. For more information about MBSA support, visit the following Microsoft Baseline Security Analyzer (MBSA) 1.2.1 Q&A.

Can I use Systems Management Server (SMS) to determine if this update is required?

Yes. SMS can help detect and deploy this security update. For information about SMS, visit the SMS Web site.

The Security Update Inventory Tool is required for detecting Microsoft Windows and other affected Microsoft products. For more information about the limitations of the Security Update Inventory Tool, see <http://support.microsoft.com/kb/306460> Microsoft Knowledge Base Article 306460.

### Mitigating Factors:

In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability (An attacker could also attempt to compromise a Web site to have it serve up a Web page with malicious content to attempt to exploit this vulnerability.). An attacker would have no way to force users to visit a Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site or to a site that has been compromised by the attacker. An attacker who successfully exploited this vulnerability could gain the same privileges as the user. Users whose accounts are configured to have fewer privileges on the system could be less impacted than users who operate with administrative privileges.

By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 2000 opens HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been installed. Outlook Express 5.5 Service Pack 2 opens HTML e-mail messages in the Restricted sites zone if

## Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

Microsoft Security Bulletin MS04-018 has been installed. The Restricted sites zone helps reduce attacks that could attempt to exploit this vulnerability.

The risk of attack from the HTML e-mail vector can be significantly reduced if you meet all the following conditions:

Install the update that is included with Microsoft Security Bulletin <<http://www.microsoft.com/technet/security/bulletin/MS03-040.msp>>

MS03-040 or a later Cumulative Security Update for Internet Explorer.

Use Microsoft Outlook 2000 with the Microsoft Outlook E-mail Security Update installed.

Use Microsoft Outlook Express 6 or later or Microsoft Outlook 2000 Service Pack 2 or later in their default configuration.

By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode mitigates this vulnerability. See the FAQ section for this security update for more information about Internet Explorer Enhanced Security Configuration.

### Workarounds:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified below.

Set Internet and Local intranet security zone settings to High to prompt before running ActiveX controls and active scripting in the Internet zone and in the Local intranet zone.

You can help protect against this vulnerability by changing your settings for the Internet security zone to prompt before running ActiveX controls and active scripting. You can do this by setting your browser security to High.

To raise the browsing security level in Microsoft Internet Explorer:

1. On the Internet Explorer Tools menu, click Internet Options.
2. In the Internet Options dialog box, click the Security tab, and then click the Internet icon.
3. Under Security level for this zone, move the slider to High. This sets the security level for all Web sites you visit to High.

Note If no slider is visible, click Default Level, and then move the slider to High.

Note Setting the level to High may cause some Web sites to work incorrectly. If you have difficulty using a Web site after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the high security setting.

Alternatively, you can change your settings to prompt before running ActiveX controls only by following these steps:

1. In Internet Explorer, click Internet Options on the Tools menu.
2. Click the Security tab.
3. Click Internet, and then click Custom Level.
4. Under Settings, in the ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt.
5. In the Scripting section, under Active Scripting, click Prompt, and then click OK.

## Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

6. Click Local intranet, and then click Custom Level.
7. Under Settings, in the ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt.
8. In the Scripting section, under Active Scripting, click Prompt.
9. Click OK two times to return to Internet Explorer.

Impact of Workaround: There are side effects to prompting before running ActiveX controls. Many Web sites that are on the Internet or on an intranet use ActiveX to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX controls to provide menus, ordering forms, or even account statements. Prompting before running ActiveX controls is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click Yes to run ActiveX controls. If you do not want to be prompted for all these sites, use the "Restrict Web sites to only your trusted Web sites" workaround.

Restrict Web sites to only your trusted Web sites.

After you set Internet Explorer to require a prompt before it runs ActiveX controls and active scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to Internet Explorer's Trusted sites zone. This will allow you to continue to use trusted Web sites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone.

To do this, follow these steps:

1. In Internet Explorer, click Tools, click Internet Options, and then click the Security tab.
2. In the Select a Web content zone to specify its current security settings box, click Trusted Sites, and then click Sites.
3. 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.
4. In the Add this Web site to the zone box, type the URL of a site that you trust, and then click Add.
5. Repeat these steps for each site that you want to add to the zone.
6. Click OK two times 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 "\*.windowsupdate.microsoft.com" (without the quotation marks). This is the site that will host the update, and it requires using an ActiveX control to install the update.

Install the

<http://www.microsoft.com/office/previous/outlook/2002security.asp>

Outlook E-mail Security Update if you are using Outlook 2000 SP1 or earlier.

## Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 2000 opens HTML e-mail messages in the Restricted sites zone if the <http://www.microsoft.com/office/outlook/evaluation/security.asp> Outlook E-mail Security Update has been installed.

Customers who use any of these products could be at a reduced risk from an e-mail-borne attack that tries to exploit this vulnerability unless the user clicks a malicious link in the e-mail message.

Install the update that is described in Microsoft Security Bulletin <http://go.microsoft.com/fwlink/?LinkId=19527> MS04-018 if you are using Outlook Express 5.5 SP2.

Outlook Express 5.5 Service Pack 2 opens HTML e-mail messages in the Restricted sites zone if Microsoft Security Bulletin <http://go.microsoft.com/fwlink/?LinkId=19527> MS04-018 has been installed.

Customers who use any of these products could be at a reduced risk from an e-mail-borne attack that tries to exploit this vulnerability unless the user clicks a malicious link in the e-mail message.

Read e-mail messages in plain text format if you are using Outlook 2002 or later, or Outlook Express 6 SP1 or later, to help protect yourself from the HTML e-mail attack vector.

Outlook 2002 users who have applied Office XP Service Pack 1 or later and Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only. Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For more information about enabling this setting in Outlook 2002, see <http://support.microsoft.com/kb/307594> Microsoft Knowledge Base Article 307594.

For information about this setting in Outlook Express 6, see <http://support.microsoft.com/kb/291387> Microsoft Knowledge Base Article 291387.

Impact of Workaround: E-mail messages that are viewed in plain text format will not contain pictures, specialized fonts, animations, or other rich content. Additionally:

- \* The changes are applied to the preview pane and to open messages.
- \* Pictures become attachments so that they are not lost.
- \* Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.

Temporarily disable the HTML Help ActiveX control from running in Internet Explorer

You can help protect against this vulnerability by temporarily disabling the HTML Help ActiveX control from running in Internet Explorer by setting the kill bit for the control.

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system.

Microsoft cannot guarantee that you can solve problems that result from

## Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

using Registry Editor incorrectly. Use Registry Editor at your own risk.

The CLSID for an ActiveX control is a GUID for that control. You can prevent an ActiveX control from running in Internet Explorer by setting the kill bit so that the control is never called by Internet Explorer. The kill bit is a specific value for the Compatibility Flags DWORD value for the ActiveX control in the registry.

The CLSID for the HTML Help ActiveX control is  
{41B23C28-488E-4E5C-ACE2-BB0BBABE99E8}

For detailed steps about stopping an ActiveX control from running in Internet Explorer, see <<http://support.microsoft.com/kb/240797>> Microsoft Knowledge Base Article 240797. Follow these steps and create a Compatibility Flags value in the registry to prevent the HTML Help ActiveX control from being instantiated in Internet Explorer

Note If you use this workaround you must reset this registry change by removing the same Compatibility Flags registry value. You should do this after you have applied this security update to regain normal functionality supplied by the HTML Help ActiveX control.

Impact of Workaround: Disabling the HTML Help ActiveX control prevents Internet Explorer from instantiating the control. This configuration causes program compatibility issues. Some examples of such issues are:

- \* In Help and Support Center, the Index feature no longer works.
- \* In HTML Help, features such as Related Topics and Shortcuts no longer work.
- \* Features that are provided by the HTML Help control in Enterprise intranet programs no longer work.

### FAQ:

What is the scope of the vulnerability?

This is a cross-domain vulnerability that could allow information disclosure or remote code execution. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system could be less impacted than users who operate with administrative privileges.

What causes the vulnerability?

The way that the HTML Help ActiveX control processes cross domain requests.

What is HTML Help?

Microsoft HTML Help is the standard help system for the Windows platform. The HTML Help ActiveX control is a program that is used to insert help navigation and secondary window functionality into an HTML file. For more information about the HTML Help ActiveX control, see the product

documentation.

What is the cross-domain security model that Internet Explorer implements?

One of the principal security functions of a browser is to make sure that browser windows that are under the control of different Web sites cannot interfere with each other or access each other's data, while allowing windows from the same site to interact with each other. To differentiate between cooperative and uncooperative browser windows, the concept of a "domain" has been created. A domain is a security boundary – any open windows within the same domain can interact with each other, but windows from different domains cannot. The cross-domain security model is the part of the security architecture that keeps windows from different domains from interfering with each other.

The simplest example of a domain is associated with Web sites. If you visit <http://www.wingtiptoy.com>, and it opens a window to <http://www.wingtiptoy.com/security>, the two windows can interact with each other because both sites belong to the same domain, <http://www.wingtiptoy.com>. However, if you visited <http://www.wingtiptoy.com>, and it opened a window to a different Web site, the cross-domain security model would help protect the two windows from each other. The concept goes even further. The file system on your local computer is also a domain. For example, <http://www.wingtiptoy.com> could open a window and show you a file on your hard disk. However, because your local file system is in a different domain from the Web site, the cross-domain security model should prevent the Web site from reading the file that is being displayed.

The Internet Explorer cross-domain security model can be configured by using the security zone settings in Internet Explorer.

What are Internet Explorer security zones?

Internet Explorer security zones are part of a system that divides online content into categories or zones that are based on the trustworthiness of the content. Specific Web domains can be assigned to a zone, depending on how much you trust the content of each domain. The zone then restricts the capabilities of the Web content, based on the zone's policy. By default, most Internet domains are treated as part of the Internet zone. By default, the policy of the Internet zone prevents scripts and other active code from accessing resources on the local system.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could run malicious script code in the Local Machine security zone in Internet Explorer. This could allow an attacker to take complete control of the affected system.

How could an attacker exploit the vulnerability?

An attacker could exploit this vulnerability by creating a malicious Web page and persuading the user to visit the page. An attacker could also attempt to compromise a Web site to have it serve up a Web page with malicious content to try to exploit this vulnerability. When the user has

## Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

visited the page, the attacker could access information from other Web sites, access local files on the system, or cause malicious script to run as the locally logged on user.

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user view Web sites for malicious action to occur. Therefore, any systems where Internet Explorer is used frequently, such as users workstations or terminal servers, are at the most risk from this vulnerability. Systems that are not typically used to visit Web sites, such as most server systems, are at a reduced risk.

Are Windows 98, Windows 98 Second Edition or Windows Millennium Edition critically affected by this vulnerability?

Yes. Windows 98, Windows 98 Second Edition, and Windows Millennium Edition are critically affected by this vulnerability. A Critical security update for these platforms is available and is provided as part of this security bulletin and can be downloaded from the Windows Update Web site. For more information about severity ratings, visit the following Web site.

Note Updates for localized versions of Microsoft Windows 98 and Microsoft Windows 98 Second Edition that are not supported by Windows Update Slovenian, Slovakian, and Thai are available for download at the following

<http://www.microsoft.com/downloads/details.aspx?FamilyId=89F5412E-B7A6-4346-B7B6-5AE7095AC6BF> download location.

What does the update do?

This update prevents the creation of an instance of the HTML Help Active X control in HTML content that is served from outside the Local Machine zone.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CAN-2004-1043.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

Yes. When the security bulletin was released, Microsoft had received information that this vulnerability was being exploited

Does applying this security update help protect customers from the code that has been published publicly that attempts to exploit this vulnerability?

Yes. This security update addresses the vulnerability that is currently being exploited. The vulnerability that has been addressed has been assigned the Common Vulnerability and Exposure number CAN-2004-1043.

### ADDITIONAL INFORMATION

Securiteam: [NT] Vulnerability in HTML Help Allows Code Execution (MS05-001)

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS05-001.msp>>

<http://www.microsoft.com/technet/security/bulletin/MS05-001.msp>

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.