

# [NT] Cumulative Security Update for Internet Explorer (MS06-072)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00011.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 13 Dec 2006 17:03:05 +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>

-----

Cumulative Security Update for Internet Explorer (MS06-072)

---

## SUMMARY

This update resolves several newly discovered vulnerabilities in Microsoft Internet Explorer. If a user is logged on with administrative user rights, an attacker who successfully exploited the most severe of these vulnerabilities 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 user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

## DETAILS

Affected Software:

- \* Microsoft Windows 2000 Service Pack 4
- \* Microsoft Windows XP Service Pack 2
- \* Microsoft Windows XP Professional x64 Edition
- \* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- \* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

\* Microsoft Windows Server 2003 x64 Edition

\*

Non-Affected Software:

\* Windows Vista

Affected Components:

\* Microsoft Internet Explorer 5.01 Service Pack 4 on Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1D28E62C-09D3-4F38-BEA3-3FC501449D29>>

Download the update

\* Microsoft Internet Explorer 6 Service Pack 1 when installed on Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3CFC32FC-85CA-4EDA-890D-5E359F5F0019>>

Download the update

\* Microsoft Internet Explorer 6 for Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8B321744-B55E-4696-8B2C-B1D31672DA06>>

Download the update

\* Microsoft Internet Explorer 6 for Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8D841D1B-D0B1-46AF-87BD-7DAA8C31AF39>>

Download the update

\* Microsoft Internet Explorer 6 for Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3E3A9693-D21B-4214-A16C-3FC22340E600>>

Download the update

\* Microsoft Internet Explorer 6 for Windows Server 2003 for Itanium-based Systems and Windows Server 2003 with SP1 for Itanium-based Systems

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9E3F7A2C-BFE1-48C5-8A8A-64A06BCDF219>>

Download the update

\* Microsoft Internet Explorer 6 for Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=F56065CE-6D28-479B-80A7-E04022454DE9>>

Download the update

Non-Affected Components:

\* Windows Internet Explorer 7 for Windows XP Service Pack 2

\* Windows Internet Explorer 7 for Windows XP Professional x64 Edition

\* Windows Internet Explorer 7 for Windows Server 2003 Service Pack 1

\* Windows Internet Explorer 7 for Windows Server 2003 with SP1 for Itanium-based Systems

\* Windows Internet Explorer 7 for Windows Server 2003 x64 Edition

\* Windows Internet Explorer 7 in Windows Vista

CVE Information:

Script Error Handling Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5579>>

CVE-2006-5579

DHTML Script Function Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5581>>

CVE-2006-5581

TIF Folder Information Disclosure Vulnerability –

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5578>>  
CVE-2006-5578

TIF Folder Information Disclosure Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5577>>  
CVE-2006-5577

Script Error Handling Memory Corruption Vulnerability – CVE-2006-5579:

A remote code execution vulnerability exists in Internet Explorer due to attempts to access previously freed memory when handling script errors in certain situations. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If a user viewed the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for Script Error Handling Memory Corruption Vulnerability – CVE-2006-5579:

In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site.

\* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

\* By default, all supported versions of Microsoft Outlook and Microsoft Outlook Express open HTML e-mail messages in the Restricted sites zone. The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing Active Scripting and ActiveX controls from being used when reading HTML e-mail. However, if a user clicks on a link within an e-mail they could still be vulnerable to this issue through the Web-based attack scenario.

\* By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as

<[http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc\\_changes.asp](http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc_changes.asp)>  
Enhanced Security Configuration. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that have not been added to Internet Explorer Trusted sites zone. See the FAQ section of this security update for more information about Internet Explorer Enhanced Security Configuration.

\* Windows Internet Explorer 7 for Windows XP Service Pack 2, Windows Internet Explorer 7 for Windows XP Professional x64 Edition, Windows

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

Internet Explorer 7 for Windows Server 2003 Service Pack 1, Windows Internet Explorer 7 for Windows Server 2003 with SP1 for Itanium-based Systems, Windows Internet Explorer 7 for Windows Server 2003 x64 Edition, and Windows Internet Explorer 7 in Windows Vista are not affected by this vulnerability.

\* Microsoft Internet Explorer 5.01 Service Pack 4 on Windows 2000 Service Pack 4 is not affected by this vulnerability.

Workarounds for Script Error Handling Memory Corruption Vulnerability – CVE-2006-5579:

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

\* Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone

You can help protect against this vulnerability by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, follow 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 Scripting section, under Active Scripting, click Prompt or Disable, and then click OK.
5. Click Local intranet, and then click Custom Level.
6. Under Settings, in the Scripting section, under Active Scripting, click Prompt or Disable, and then click OK.
7. Click OK two times to return to Internet Explorer.

Note Disabling Active Scripting in the Internet and Local intranet security zones 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.

Impact of Workaround: There are side effects to prompting before running Active Scripting. Many Web sites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements.

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

Prompting before running Active Scripting 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 Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone .

Add sites that you trust to the Internet Explorer Trusted sites zone

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 the Internet Explorer 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.

Note Add any sites that you trust not to take malicious action on your computer. Two in particular that you may want to add are "\*.windowsupdate.microsoft.com" and \*.update.microsoft.com (without the quotation marks). These are the sites that will host the update, and it requires an ActiveX Control to install the update.

\* Set Internet and Local intranet security zone settings to High to prompt before running ActiveX Controls and Active Scripting in these zones

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

To raise the browsing security level in Microsoft Internet Explorer,

follow these steps:

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 security setting set to High.

Impact of Workaround: There are side effects to prompting before running ActiveX Controls and Active Scripting. Many Web sites that are on the Internet or on an intranet use ActiveX or Active Scripting 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 or Active Scripting 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 or Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone .

Add sites that you trust to the Internet Explorer Trusted sites zone

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 the Internet Explorer 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,

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

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.

Note Add any sites that you trust not to take malicious action on your computer. Two in particular that you may want to add are "\*.windowsupdate.microsoft.com" and \*.update.microsoft.com (without the quotation marks). These are the sites that will host the update, and it requires an ActiveX Control to install the update.

FAQ for Script Error Handling Memory Corruption Vulnerability – CVE-2006-5579:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could remotely take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

If a user is logged on with administrative user rights, 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 user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

What causes the vulnerability?

Internet Explorer attempts to access previously freed memory when handling script errors in certain situations. As a result, system memory may be corrupted in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

How could an attacker exploit the vulnerability?

An attacker could host a specially crafted Web site that is designed to exploit these vulnerabilities through Internet Explorer and then persuade a user to view the Web site. This can also include Web sites that accept user-provided content or advertisements, Web sites that host user-provided content or advertisements, and compromised Web sites. These Web sites

could contain specially crafted content that could exploit these vulnerabilities. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or in an Instant Messenger message that takes users to the attacker's Web site. It could also be possible to display specially crafted Web content by using banner advertisements or by using other methods to deliver Web content to affected systems.

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user is logged on and visits a Web site for any malicious action to occur. Therefore, any systems where Internet Explorer is used frequently, such as workstations or terminal servers, are at the most risk from these vulnerabilities.

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

Yes. By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that have not been added to Internet Explorer Trusted sites zone.

What is the Internet Explorer Enhanced Security Configuration?

Internet Explorer

<[http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc\\_changes.asp](http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc_changes.asp)>

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 specially crafted Web content on a server. Internet Explorer Enhanced Security Configuration reduces this risk by modifying many security-related settings. This includes the settings on the Security tab 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), 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 and prevents non-Microsoft extensions from running.
- \* Multimedia content is disabled. This setting prevents music, animations, and video clips from running.

For more information regarding Internet Explorer Enhanced Security Configuration, see the guide, Managing Internet Explorer Enhanced Security Configuration, at the following

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

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

What does the update do?

The update removes the vulnerability by modifying the script error exception handling so that there is no attempt made to access the freed memory.

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

No. Microsoft received information about this vulnerability through responsible disclosure.

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

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

### DHTML Script Function Memory Corruption Vulnerability – CVE-2006-5581:

A remote code execution vulnerability exists in the way Internet Explorer interprets certain DHTML script function calls to incorrectly created elements. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user viewed the Web page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

### Mitigating Factors for DHTML Script Function Memory Corruption Vulnerability – CVE-2006-5581:

\* In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites.

Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site.

\* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

\* By default, all supported versions of Microsoft Outlook and Microsoft Outlook Express open HTML e-mail messages in the Restricted sites zone. The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing Active Scripting and ActiveX controls from being used when reading HTML e-mail. However, if a user clicks on a link within an e-mail they could still be vulnerable to this issue through the Web-based attack scenario.

\* By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as

[http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc\\_changes.asp](http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc_changes.asp)

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

Enhanced Security Configuration. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that have not been added to Internet Explorer Trusted sites zone. See the FAQ section of this security update for more information about Internet Explorer Enhanced Security Configuration.

\* Windows Internet Explorer 7 for Windows XP Service Pack 2, Windows Internet Explorer 7 for Windows XP Professional x64 Edition, Windows Internet Explorer 7 for Windows Server 2003 Service Pack 1, Windows Internet Explorer 7 for Windows Server 2003 with SP1 for Itanium-based Systems, Windows Internet Explorer 7 for Windows Server 2003 x64 Edition, and Windows Internet Explorer 7 in Windows Vista are not affected by this vulnerability.

\* Microsoft Internet Explorer 5.01 Service Pack 4 on Windows 2000 Service Pack 4 is not affected by this vulnerability.

Workarounds for DHTML Script Function Memory Corruption Vulnerability – CVE-2006-5581:

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

\* Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone

You can help protect against this vulnerability by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, follow 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 Scripting section, under Active Scripting, click Prompt or Disable, and then click OK.
5. Click Local intranet, and then click Custom Level.
6. Under Settings, in the Scripting section, under Active Scripting, click Prompt or Disable, and then click OK.
7. Click OK two times to return to Internet Explorer.

Note Disabling Active Scripting in the Internet and Local intranet security zones 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.

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

Impact of Workaround: There are side effects to prompting before running Active Scripting. Many Web sites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting 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 Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone .

Add sites that you trust to the Internet Explorer Trusted sites zone.

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 the Internet Explorer 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.

Note Add any sites that you trust not to take malicious action on your computer. Two in particular that you may want to add are "\*.windowsupdate.microsoft.com" and \*.update.microsoft.com (without the quotation marks). These are the sites that will host the update, and it requires an ActiveX Control to install the update.

\* Set Internet and Local intranet security zone settings to High to prompt before running ActiveX Controls and Active Scripting in these zones

You can help protect against this vulnerability by changing your settings

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

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, follow these steps:

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 security setting set to High.

Impact of Workaround: There are side effects to prompting before running ActiveX Controls and Active Scripting. Many Web sites that are on the Internet or on an intranet use ActiveX or Active Scripting 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 or Active Scripting 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 or Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone

Add sites that you trust to the Internet Explorer Trusted sites zone.

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 the Internet Explorer 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.

Note Add any sites that you trust not to take malicious action on your computer. Two in particular that you may want to add are "\*.windowsupdate.microsoft.com" and \*.update.microsoft.com (without the quotation marks). These are the sites that will host the update, and it requires an ActiveX Control to install the update.

FAQ for DHTML Script Function Memory Corruption Vulnerability – CVE-2006-5581:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could remotely take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

If a user is logged on with administrative user rights, 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 user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

What causes the vulnerability?

When Internet Explorer interprets certain DHTML script function calls to incorrectly created elements it may corrupt system memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

How could an attacker exploit the vulnerability?

An attacker could host a specially crafted Web site that is designed to exploit these vulnerabilities through Internet Explorer and then persuade

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

a user to view the Web site. This can also include Web sites that accept user-provided content or advertisements, Web sites that host user-provided content or advertisements, and compromised Web sites. These Web sites could contain specially crafted content that could exploit these vulnerabilities. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or in an Instant Messenger message that takes users to the attacker's Web site. It could also be possible to display specially crafted Web content by using banner advertisements or by using other methods to deliver Web content to affected systems.

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user is logged on and visits a Web site for any malicious action to occur. Therefore, any systems where Internet Explorer is used frequently, such as workstations or terminal servers, are at the most risk from these vulnerabilities.

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

Yes. By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that have not been added to Internet Explorer Trusted sites zone.

What is the Internet Explorer Enhanced Security Configuration?

Internet Explorer

[http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc\\_changes.asp](http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc_changes.asp)

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 specially crafted Web content on a server. Internet Explorer Enhanced Security Configuration reduces this risk by modifying many security-related settings. This includes the settings on the Security tab 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), 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 and prevents non-Microsoft extensions from running.
- \* Multimedia content is disabled. This setting prevents music, animations, and video clips from running.

For more information regarding Internet Explorer Enhanced Security Configuration, see the guide, Managing Internet Explorer Enhanced Security Configuration, at the following

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

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

What does the update do?

The update removes the vulnerability by modifying the way that Internet Explorer handles the DHTML script function call.

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

No. Microsoft received information about this vulnerability through responsible disclosure.

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

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

### TIF Folder Information Disclosure Vulnerability – CVE-2006-5578

An information disclosure vulnerability exists in Internet Explorer in the way that drag and drop operations are handled in certain situations. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow for information disclosure if a user viewed and interacted with the Web page. An attacker who successfully exploited this vulnerability would be able to retrieve files from the Temporary Internet Files (TIF) folder on a user's system.

### Mitigating Factors for TIF Folder Information Disclosure Vulnerability – CVE-2006-5578:

- \* User interaction is required to exploit this vulnerability.
- \* In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit these vulnerabilities. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit these vulnerabilities. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site.
- \* By default, all supported versions of Microsoft Outlook and Microsoft Outlook Express open HTML e-mail messages in the Restricted sites zone. The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing Active Scripting and ActiveX controls from being used when reading HTML e-mail. However, if a user clicks on a link within an e-mail they could still be vulnerable to this issue through the Web-based attack scenario.
- \* By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that have not been added to Internet

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

Explorer Trusted sites zone. See the FAQ section of this security update for more information about Internet Explorer Enhanced Security Configuration.

\* Windows Internet Explorer 7 for Windows XP Service Pack 2, Windows Internet Explorer 7 for Windows XP Professional x64 Edition, Windows Internet Explorer 7 for Windows Server 2003 Service Pack 1, Windows Internet Explorer 7 for Windows Server 2003 with SP1 for Itanium-based Systems, Windows Internet Explorer 7 for Windows Server 2003 x64 Edition, and Windows Internet Explorer 7 in Windows Vista are not affected by this vulnerability.

Workarounds for TIF Folder Information Disclosure Vulnerability – CVE-2006-5578:

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

\* Disable Drag and Drop or copy and paste files in Internet Explorer  
Disable the Drag and drop or copy and paste files option in the Internet and intranet zones. To do this, follow these steps:

1. In Internet Explorer, click Internet Options on the Tools menu, and then click the Security tab.
2. In the Select a Web content zone to specify its security settings box, click Internet, and then click Custom Level.
3. In the Settings box, locate the Drag and drop or copy and paste files option under Miscellaneous. Make a note of your current setting.
4. Under Drag and drop or copy and paste files, click Disable, and then click OK.
5. Click Yes, and then click OK two times.

Note Repeat these steps for the local intranet zone by clicking Local intranet instead of Internet in step 2.

\* Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone

You can help protect against this vulnerability by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, follow 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 Scripting section, under Active Scripting, click Prompt or Disable, and then click OK.
5. Click Local intranet, and then click Custom Level.
6. Under Settings, in the Scripting section, under Active Scripting, click Prompt or Disable, and then click OK.
7. Click OK two times to return to Internet Explorer.

Note Disabling Active Scripting in the Internet and Local intranet security zones 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.

Impact of Workaround: There are side effects to prompting before running Active Scripting. Many Web sites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting 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 Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone .

#### Add sites that you trust to the Internet Explorer Trusted sites zone

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 the Internet Explorer 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.

Note Add any sites that you trust not to take malicious action on your computer. Two in particular that you may want to add are "\*.windowsupdate.microsoft.com" and \*.update.microsoft.com (without the quotation marks). These are the sites that will host the update, and it requires an ActiveX Control to install the update.

\* Set Internet and Local intranet security zone settings to High to prompt before running ActiveX Controls and Active Scripting in these zones

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

To raise the browsing security level in Microsoft Internet Explorer, follow these steps:

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 security setting set to High.

Impact of Workaround: There are side effects to prompting before running ActiveX Controls and Active Scripting. Many Web sites that are on the Internet or on an intranet use ActiveX or Active Scripting 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 or Active Scripting is a global setting that affects all Internet and

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

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 or Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone .

\* Add sites that you trust to the Internet Explorer Trusted sites zone

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 the Internet Explorer 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.

Note Add any sites that you trust not to take malicious action on your computer. Two in particular that you may want to add are "\*.windowsupdate.microsoft.com" and \*.update.microsoft.com (without the quotation marks). These are the sites that will host the update, and it requires an ActiveX Control to install the update.

FAQ for TIF Folder Information Disclosure Vulnerability – CVE-2006-5578:

What is the scope of the vulnerability?

This is an information disclosure vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow for information disclosure of cached content in the Temporary Internet Files (TIF) folder if a user viewed and interacted with the Web page.

What causes the vulnerability?

The vulnerability is a result of how Internet Explorer handles drag and drop operations in certain situations.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability would be able to retrieve files from the Temporary Internet Files (TIF) folder on a user's system.

How could an attacker exploit the vulnerability?

An attacker could host a specially crafted Web site that is designed to exploit this vulnerability through Internet Explorer and then persuade a user to view the Web site. This can also include Web sites that accept user-provided content or advertisements, Web sites that host user-provided content or advertisements, and compromised Web sites. These Web sites could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or in an Instant Messenger message that takes users to the attacker's Web site. It could also be possible to display specially crafted Web content by using banner advertisements or by using other methods to deliver Web content to affected systems.

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user is logged on and visits a Web site for any malicious action to occur. Therefore, any systems where Internet Explorer is used frequently, such as workstations or terminal servers, are at the most risk from this vulnerability.

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

Yes. By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that have not been added to Internet Explorer Trusted sites zone.

What is the Internet Explorer Enhanced Security Configuration?

Internet Explorer

<[http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc\\_changes.asp](http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc_changes.asp)>

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 specially crafted Web content on a server. Internet Explorer Enhanced Security Configuration reduces this risk by modifying many security-related settings. This includes the settings on the Security tab 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), and file downloads.

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

\* 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 and prevents non-Microsoft extensions from running.

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

For more information regarding Internet Explorer Enhanced Security Configuration, see the guide, *Managing Internet Explorer Enhanced Security Configuration*, at the following

[http://www.microsoft.com/downloads/details.aspx?FamilyID=d41b036c-e2e1-4960-99bb-9757f7e9e31b&Display=Web site](http://www.microsoft.com/downloads/details.aspx?FamilyID=d41b036c-e2e1-4960-99bb-9757f7e9e31b&Display=Web%20site).

What does the update do?

The update removes the vulnerability by ensuring that a drag and drop operation does not expose the location of the cached content in the TIF folder.

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

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

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

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

TIF Folder Information Disclosure Vulnerability – CVE-2006-5577:

An information disclosure vulnerability exists in Internet Explorer in certain scenarios where the path to the cached content in the TIF folder could be disclosed. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow for information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability would be able to retrieve files from the Temporary Internet Files (TIF) folder on a user's system. However, user interaction is required to exploit this vulnerability.

Mitigating Factors for TIF Folder Information Disclosure Vulnerability – CSV-2006-5577:

\* In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit these vulnerabilities. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

content that could exploit these vulnerabilities. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site.

\* By default, all supported versions of Microsoft Outlook and Microsoft Outlook Express open HTML e-mail messages in the Restricted sites zone. The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing Active Scripting and ActiveX controls from being used when reading HTML e-mail. However, if a user clicks on a link within an e-mail they could still be vulnerable to this issue through the Web-based attack scenario.

\* By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that have not been added to Internet Explorer Trusted sites zone. See the FAQ section of this security update for more information about Internet Explorer  
<[http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc\\_changes.asp](http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc_changes.asp)>  
Enhanced Security Configuration.

\* Windows Internet Explorer 7 for Windows XP Service Pack 2, Windows Internet Explorer 7 for Windows XP Professional x64 Edition, Windows Internet Explorer 7 for Windows Server 2003 Service Pack 1, Windows Internet Explorer 7 for Windows Server 2003 with SP1 for Itanium-based Systems, Windows Internet Explorer 7 for Windows Server 2003 x64 Edition, and Windows Internet Explorer 7 in Windows Vista are not affected by this vulnerability.

Workarounds for TIF Folder Information Disclosure Vulnerability –  
CVE-2006-5577:

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

\* Configure Internet Explorer to prompt before running ActiveX Controls or disable ActiveX Controls in the Internet and Local intranet security zone

You can help protect against these vulnerabilities by changing your Internet Explorer settings to prompt before running ActiveX controls. To do this, follow these steps:

1. In Internet Explorer, click Internet Options on the Tools menu.
2. Click the Security tab.

## [NT] Cumulative Security Update for Internet Explorer (MS06-072)

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 or Disable, and then click OK.
5. Click Local intranet, and then click Custom Level.
6. Under Settings, in the ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt or Disable, and then click OK.
7. 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 t