

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-04/msg00021.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 18 Apr 2006 12:38:57 +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 (MS06-013)

SUMMARY

Multiple remote code execution, information disclosure and Spoofing in Microsoft Internet Explorer allow attackers to execute arbitrary code, retrieve information and spoof the user UI.

DETAILS

Vulnerable Systems:

- * Microsoft Windows 2000 Service Pack 4
- * Microsoft Windows XP Service Pack 1 and 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 Service Pack 1 for Itanium-based Systems
- * Microsoft Windows Server 2003 x64 Edition family
- * 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.

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

Note The security updates for Microsoft Windows Server 2003, Microsoft Windows Server 2003 Service Pack 1, and Microsoft Windows Server 2003 x64 Edition also apply to Microsoft Windows Server 2003 R2.

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=594E7B87-AF8F-4346-9164-596E3E5C22B1>>

Download the update

* Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 4 or on Microsoft Windows XP Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=033C41E1-2B36-4696-987A-099FC57E0129>>

Download the update

* Internet Explorer 6 for Microsoft Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=F05FFB31-E6B4-4771-81F1-4ACCEBF72133>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=EE566871-D217-41D3-BECC-B27FAFA00054>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E584957C-0ABE-4129-ABAF-AA2852AD62A3>>

Download the update

* Internet Explorer 6 for Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=5A1C8BE3-39EE-4937-9BD1-280FC35125C6>>

Download the update

* Internet Explorer 6 for Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C278FE3E-620A-4BBC-868B-CA2D9EFF7AC3>>

Download the update

* Internet Explorer 6 Service Pack 1 on Microsoft Windows 98, on Microsoft Windows 98 SE, or on Microsoft Windows Millennium Edition
Review the FAQ section of this bulletin for details about this version.

DHTML Method Call Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1359>>

CVE-2006-1359:

A remote code execution vulnerability exists in the way Internet Explorer displays a Web page that contains certain unexpected method calls to HTML objects. As a result, system memory may be corrupted in such a way that an attacker could execute arbitrary code if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for DHTML Method Call Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1359>>

CVE-2006-1359:

* 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 would have no way to force users to visit a malicious 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 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.

* The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing Active Scripting from being used when reading HTML e-mail messages. However, if a user clicks a link in an e-mail message, they could still be vulnerable to this issue through the Web-based attack scenario.

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://go.microsoft.com/fwlink/?LinkId=33334>> 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 Microsoft Security Bulletin <<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 has been installed.

* 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> Enhanced Security Configuration. This mode mitigates this vulnerability in the e-mail vector because reading e-mail messages in plain text is the default configuration for Outlook Express. See the FAQ section of this security update for more information about Internet Explorer Enhanced Security Configuration.

Workarounds for DHTML Method Call Memory Corruption Vulnerability – <<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1359>> CVE-2006-1359:

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 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.

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

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 Internet Explorer's Trusted sites zone .

Add sites that you trust to Internet Explorer's 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 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.

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

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 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 Internet Explorer's Trusted sites zone

Add sites that you trust to Internet Explorer's 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 Internet Explorer's

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

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> 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 Method Call Memory Corruption Vulnerability –
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1359>>
CVE-2006-1359:

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.

What causes the vulnerability?

When Internet Explorer displays a Web page that contains certain unexpected method calls to HTML objects, system memory may be corrupted in such a way that an attacker could execute arbitrary code.

Specifically, the public postings discuss a potential behavior in Internet Explorer in the way that HTML objects may handle an unexpected createTextRange() method call to an HTML object. A Web page that is specially crafted to exploit this vulnerability will cause Internet Explorer to fail. As a result of this, system memory may be corrupted in such a way that an attacker could execute arbitrary code.

What is the createTextRange() method?

The createTextRange() method is a dynamic HTML (DHTML) method that is exposed by the DHTML Object Model. For more information about DHTML

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

methods, visit the

<<http://msdn.microsoft.com/library/default.asp?url=/workshop/author/dhtml/reference/methods.asp>> MSDN Library Web site.

What might an attacker use the vulnerability to do?

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.

How could an attacker exploit the vulnerability?

An attacker could host a malicious 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 malicious 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 request 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.

Could this vulnerability be exploited through e-mail?

This vulnerability could not be exploited automatically through e-mail or while viewing e-mail messages in the preview pane while using Outlook or Outlook Express. Customers would have to click on a link that would take them to a malicious Web site, or open an attachment that could exploit the vulnerability.

What systems are primarily at risk from the vulnerability?

This vulnerability requires a user to be logged on and visiting 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.

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. The security updates are available from the <<http://go.microsoft.com/fwlink/?LinkId=21130>> Windows Update Web site. For more information about severity ratings, visit the following <<http://go.microsoft.com/fwlink/?LinkId=21140>> Web site.

What does the update do?

The update removes the vulnerability by changing the way that Internet Explorer initializes memory before using it.

When this security bulletin was issued, had this vulnerability been

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

publicly disclosed?

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CVE-2006-1359.

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 CVE-2006-1359.

Multiple Event Handler Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1245>>
CVE-2006-1245:

A remote code execution vulnerability exists in the way Internet Explorer handles multiple event handlers in an HTML element. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for Multiple Event Handler Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1245>>
CVE-2006-1245:

* 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 would have no way to force users to visit a malicious 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 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, 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>
Enhanced Security Configuration. This mode mitigates this vulnerability in the e-mail vector because reading e-mail messages in plain text is the default configuration for Outlook Express. See the FAQ section of this security update for more information about Internet Explorer Enhanced Security Configuration.

Workarounds for Multiple Event Handler Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1245>>

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

CVE-2006-1245:

No workarounds have been identified for this vulnerability.

FAQ for Multiple Event Handler Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1245>>

CVE-2006-1245:

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.

What causes the vulnerability?

When Internet Explorer handles multiple event handlers in an HTML element, system memory may be corrupted in such a way that an attacker could execute arbitrary code.

For example, when Internet Explorer displays a Web page that contains multiple onLoad events in an HTML element, 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 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.

How could an attacker exploit the vulnerability?

An attacker could host a malicious 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 malicious 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 request 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 reading HTML e-mail messages or that a user is logged on and visits a Web site for any malicious action to occur. Therefore, any systems where HTML e-mail messages are read or where Internet Explorer is used frequently, such as workstations or terminal servers, are at the most risk from this vulnerability.

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

Note The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing Active Scripting from being used when reading HTML e-mail messages. However, if a user clicks a link in an e-mail message, they could still be vulnerable to this issue through the Web-based attack scenario. It may be possible to exploit this vulnerability without making use of Active Scripting. However, our investigation has shown that this is harder to exploit without the use of Active Scripting.

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. The security updates are available from the <http://go.microsoft.com/fwlink/?LinkId=21130> Windows Update Web site. For more information about severity ratings, visit the following <http://go.microsoft.com/fwlink/?LinkId=21140> Web site.

What does the update do?

The update removes the vulnerability by modifying the way that Internet Explorer handles multiple event handlers so that Internet Explorer does not exit in an exploitable way.

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 CVE-2006-1245.

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

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

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 potentially could be exploited by using the published proof of concept code. The vulnerability that has been addressed has been assigned the Common Vulnerability and Exposure number CVE-2006-1245.

HTA Execution Vulnerability –

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1388>
CVE-2006-1388:

A remote code execution vulnerability exists in Internet Explorer. An HTML Application (HTA) can be initiated in a way that bypasses the security control within Internet Explorer. This allows an HTA to execute without Internet Explorer displaying the normal security dialog box. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for HTA Execution Vulnerability – CVE-2006-1388:

* 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 would have no way to force users to visit a malicious 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 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.

* The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing Active Scripting from being used when reading HTML e-mail messages. However, if a user clicks a link in an e-mail message, they could still be vulnerable to this issue through the Web-based attack scenario.

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://go.microsoft.com/fwlink/?LinkId=33334> 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 Microsoft Security Bulletin <http://go.microsoft.com/fwlink/?LinkId=19527> MS04-018 has been installed.

* 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 Enhanced Security Configuration. This mode mitigates this vulnerability. See the FAQ section of this security update for more information about Internet Explorer Enhanced Security Configuration.

Workarounds for HTA Execution Vulnerability –

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1388>
CVE-2006-1388:

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 in the following section.

* Un-register the Mshta.exe file

To un-register the Mshta.exe file, use the following command:

Click Start, click Run, type ""% windir%\system32\mshta.exe /unregister" (without the quotation marks), and then click OK.

Impact of Workaround: Users will be prompted to select a software to open HTML Applications (.HTA files) with.

To undo this change, re-register Mshta.exe by following the above steps. Replace the text in Step 1 with ""%windir%\system32\mshta.exe /register" (without the quotation marks).

* Modify the Access Control List on the Mshta.exe file

You can help protect against this vulnerability by modifying the Access Control List on the Mshta.exe file. To do this, follow these steps:

1. Click Start, click Run, type "cmd" (without the quotation marks), and then click OK.
2. Type the following command at a command prompt. Make a note of the current ACLs that are on the file (including inheritance settings) for future reference to undo this modification:
cacls %windir%\system32\mshta.exe
3. Type the following command at a command prompt to deny the everyone group access to this file:
cacls %windir%\system32\mshta.exe /d everyone

Impact of Workaround: HTML Applications (.HTA files) will stop working.

* Configure Internet Explorer to prompt before running Active Scripting or 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

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

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 Internet Explorer's Trusted sites zone .

Add sites that you trust to Internet Explorer's 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 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.

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 Internet Explorer's Trusted sites zone

Add sites that you trust to Internet Explorer's 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 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.

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 HTA Execution Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1388>>

CVE-2006-1388:

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.

What causes the vulnerability?

An HTML Application (HTA) can be initiated in a way that bypasses the security control within Internet Explorer. This allows an HTA to execute without Internet Explorer displaying the normal security dialog box.

What might an attacker use the vulnerability to do?

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.

How could an attacker exploit the vulnerability?

An attacker could host a malicious 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 malicious 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 request 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 a user to be logged on and visiting 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.

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

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. The security updates are available from the <<http://go.microsoft.com/fwlink/?LinkId=21130>> Windows Update Web site. For more information about severity ratings, visit the following <<http://go.microsoft.com/fwlink/?LinkId=21140>> Web site.

What does the update do?

The update removes the vulnerability by changing Internet Explorer so that the appropriate security dialog is displayed.

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.

HTML Parsing Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1185>>
CVE-2006-1185:

A remote code execution vulnerability exists in the way Internet Explorer handles specially crafted and not valid HTML. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for HTML Parsing Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1185>>
CVE-2006-1185:

* 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 would have no way to force users to visit a malicious 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 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, Internet Explorer on Windows Server 2003 runs in a

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

restricted mode that is known as

<http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc_changes.asp>

Enhanced Security Configuration. This mode mitigates this vulnerability in the e-mail vector because reading e-mail messages in plain text is the default configuration for Outlook Express. See the FAQ section of this security update for more information about Internet Explorer Enhanced Security Configuration.

* This vulnerability does not affect Internet Explorer 6 Service Pack 1 on Windows XP Service Pack 1, Windows 2000 Service Pack 4, Windows 98, Windows 98 Second Edition (SE), or Windows Millennium Edition (ME).

Workarounds for HTML Parsing Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1185>>

CVE-2006-1185:

No workarounds have been identified for this vulnerability.

FAQ for HTML Parsing Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1185>>

CVE-2006-1185:

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.

What causes the vulnerability?

When Internet Explorer handles specially crafted and not valid HTML 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 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.

How could an attacker exploit the vulnerability?

An attacker could host a malicious 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 malicious 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 request 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 reading HTML e-mail messages or that a user is logged on and visits a Web site for any malicious action to occur. Therefore, any systems where HTML e-mail messages are read or where Internet Explorer is used frequently, such as workstations or terminal servers, are at the most risk from this vulnerability.

What does the update do?

The update removes the vulnerability by modifying the way that Internet Explorer handles the reported specially crafted and not valid HTML.

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.

COM Object Instantiation Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1186>>
CVE-2006-1186:

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for COM Object Instantiation Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1186>>
CVE-2006-1186:

* Customers who have installed the security update included with Microsoft Security Bulletin

<<http://go.microsoft.com/fwlink/?LinkId=50690>> MS05-052 or a later security bulletin for Internet Explorer are not at risk from attacks originating from the Internet zone.

* 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 would have no way to force users to visit a malicious 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 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.

* The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing ActiveX Controls from being used when reading HTML e-mail messages. However, if a user clicks a link in an e-mail message, they could still be vulnerable to this issue through the Web-based attack scenario.

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://go.microsoft.com/fwlink/?LinkId=33334> 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 Microsoft Security Bulletin <http://go.microsoft.com/fwlink/?LinkId=19527> MS04-018 has been installed.

* 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 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 for COM Object Instantiation Memory Corruption Vulnerability – <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1186> CVE-2006-1186:

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 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 this vulnerability 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.
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.

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

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 to be prompted for all these sites, use the steps outlined in "Add sites that you trust to Internet Explorer's Trusted sites zone .

Add sites that you trust to Internet Explorer's 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 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.

<Note> 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

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

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

<Note> 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:> 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 steps outlined in "Add sites that you trust to Internet Explorer's Trusted sites zone .

Add sites that you trust to Internet Explorer's 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 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. 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 Execution Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1190>>
CVE-2006-1190:

What is the scope of the vulnerability?

A vulnerability exists in Internet Explorer that could potentially allow remote code execution or information disclosure. An attacker who successfully exploited this could at worst 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.

What causes the vulnerability?

Internet Explorer may return erroneous IOleClientSite information when an embedded object is dynamically created. This could allow this object to use the IOleClientSite information returned to make an incorrect security related decision and run in the context of the wrong site or the wrong Internet Explorer security zone.

What is IOleClientSite?

The IOleClientSite interface is the primary means by which an embedded object obtains information about the location and extent of its display site, its moniker, its user interface, and other resources provided by its container. For more information, see the <http://msdn.microsoft.com/library/en-us/com/htm/oin_oc_512d.asp> product documentation.

What are Internet Explorer security zones?

Internet Explorer

<<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q174360>> security zones are part of a system that divides online content into categories or zones, based on the trustworthiness of the content. Specific Web domains can be assigned to a zone, depending on how much trust is put in 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 gain the same user rights as the local user. Users whose accounts are configured to

[NT] Cumulative Security Update for Internet Explorer (MS06-013)

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 malicious 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 malicious 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 request 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 v