

# [NT] Cumulative Security Update for Internet Explorer (MS04-038)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0050.html>

---

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

**Date:** 10/13/04

To: list@securiteam.com

Date: 13 Oct 2004 18:20:45 +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 (MS04-038)

---

## SUMMARY

The following advisory provides details on the following vulnerabilities: CSS Heap Memory Corruption Vulnerability, Similar Method Name Redirection Cross Domain Vulnerability, Install Engine Vulnerability, Drag and Drop Vulnerability, Address Bar Spoofing on Double Byte Character Set Systems Vulnerability, Plug-in Navigation Address Bar Spoofing Vulnerability, Script in Image Tag File Download Vulnerability, and SSL Caching Vulnerability.

## DETAILS

Affected Software:

Microsoft Windows NT Server 4.0 Service Pack 6a

Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4

Microsoft Windows XP, Microsoft Windows XP Service Pack 1, and Microsoft Windows XP Service Pack 2

Microsoft Windows XP 64-Bit Edition Service Pack 1

Microsoft Windows XP 64-Bit Edition Version 2003

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

Microsoft Windows Server 2003

Microsoft Windows Server 2003 64-Bit Edition

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.

### Affected Components:

Internet Explorer 5.01 Service Pack 3 on Windows 2000 SP3:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=2D8E8E97-4946-4994-924B-1FB1DC1881BA&disp>

Download the update.

Internet Explorer 5.01 Service Pack 4 on Windows 2000 SP4:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=72DBE239-AF0A-42B5-B88C-A00371F6EC81&disp>

Download the update.

Internet Explorer 5.5 Service Pack 2 on Microsoft Windows Me:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=BE27F77C-3C2D-45F1-86DF-2B71799DA169&disp>

Download the update.

Internet Explorer 6 on Windows XP:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=A89CFBE8-C299-415D-A9D6-7CC6429C547D&disp>

Download the update.

Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 3, on Microsoft Windows 2000 Service Pack 4, on Microsoft Windows XP, or on Microsoft Windows XP Service Pack 1:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=7C1404E6-F5D4-4FED-9573-DD83F2DFF074&disp>

Download the update.

Internet Explorer 6 Service Pack 1 on Microsoft Windows NT Server 4.0

Service Pack 6a, on Microsoft Windows NT Server 4.0 Terminal Service

Edition Service Pack 6, on Microsoft Windows 98, on Microsoft Windows 98

SE, or on Microsoft Windows Me:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=DE8D94C4-7F58-4CE7-B8BD-51CFD795B03E&disp>

Download the update.

Internet Explorer 6 for Windows XP Service Pack 1 (64-Bit Edition):

<http://www.microsoft.com/downloads/details.aspx?FamilyId=C05103E8-4402-4D54-BA03-FBBC24142E4D&disp>

Download the update.

Internet Explorer 6 for Windows Server 2003:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=19E69E5F-9C98-49AD-A61F-4F82A4014412&disp>

Download the update.

Internet Explorer 6 for Windows Server 2003 64-Bit Edition and Windows XP

64-Bit Edition Version 2003:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=566C2A05-2513-4E30-A3EA-87D4BF7F9730&disp>

Download the update.

Internet Explorer 6 for Windows XP Service Pack 2:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=CF47B515-3F51-43E1-9246-2C2264C49E2E&disp>

Download the update.

The following products are not affected by this vulnerability:

Internet Explorer 6 on Windows XP Service Pack 2

Caveats: <http://support.microsoft.com/?id=834707> Microsoft Knowledge Base Article 834707 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues.

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

### CVE Information:

- \* Cascading Style Sheets (CSS) Heap Memory Corruption Vulnerability –  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0842>>  
CAN-2004-0842
- \* Similar Method Name Redirection Cross Domain Vulnerability –  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0727>>  
CAN-2004-0727
- \* Install Engine Vulnerability –  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0216>>  
CAN-2004-0216
- \* Drag and Drop Vulnerability –  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0839>>  
CAN-2004-0839
- \* Address Bar Spoofing on Double Byte Character Set Locale Vulnerability –  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0844>>  
CAN-2004-0844
- \* Plug-in Navigation Address Bar Spoofing Vulnerability –  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0843>>  
CAN-2004-0843
- \* Script in Image Tag File Download Vulnerability –  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0841>>  
CAN-2004-0841
- \* SSL Caching Vulnerability –  
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0845>>  
CAN-2004-0845

### Mitigating Factors for CSS Heap Memory Corruption Vulnerability:

- \* 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 site. After they click the link, they would be prompted to perform several actions. An attack could only occur after they performed these actions.
  - \* An attacker who successfully exploited this vulnerability could gain the same privileges as the user. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.
  - \* By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the <<http://www.microsoft.com/office/outlook/evaluation/security.asp>> Outlook E-mail Security Update has been installed. Outlook Express 5.5 Service Pack 2 opens HTML e-mail in the Restricted sites zone if Microsoft Security Bulletin <<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 has been installed. The Restricted sites zone helps reduce attacks that could attempt to exploit this vulnerability.
- The risk of attack from the HTML e-mail vector can be significantly reduced if you meet all the following conditions:
- \* Install the update that is included with Microsoft Security Bulletin

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

<<http://www.microsoft.com/technet/security/bulletin/MS03-040.msp>>

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

\* Use Outlook Express 5.5 Service Pack 2 or later and have applied the update that is included with Microsoft Security Bulletin

<<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 or a later Cumulative Security Update for Outlook Express.

\* Use Microsoft Outlook 98 and Outlook 2000 with the Microsoft Outlook E-mail Security Update installed

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

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

Workarounds for CSS Heap Memory Corruption Vulnerability:

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

Set Internet and Local Intranet security zone settings to High to prompt before running ActiveX control and Active scripting in the Internet zone and in the Local Intranet zone.

You can help protect against these vulnerabilities by changing your settings for the Internet security zone to prompt before running ActiveX controls and Active scripting. 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 click Custom Level.
4. Under Run ActiveX controls and plug-ins in the ActiveX controls and plug-ins section, click Prompt.
5. Under Active Scripting in the Scripting section, click Prompt, and then click OK.
6. Click Local intranet, and then click Custom Level.
7. Under Run ActiveX controls and plug-ins in the ActiveX controls and plug-ins section, click Prompt.
8. Under Active Scripting in the Scripting section, , click Prompt.
9. Click OK two times to return to Internet Explorer.

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

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

Restrict Web sites to only your trusted Web sites:

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

To do this follow these steps:

1. In Internet Explorer, click Tools, click Internet Options, and then click the Security tab.
2. In the Select a Web content zone to specify its current security settings box, click Trusted Sites, and then click Sites.
3. If you want to add sites that do not require an encrypted channel, click to clear the Require server verification (https:) for all sites in this zone check box.
4. In the Add this Web site to the zone box, type the URL of a site that you trust, and then click Add.
5. Repeat these steps for each site that you want to add to the zone.
6. Click OK two times to accept the changes and return to Internet Explorer.

Add any sites that you trust not to take malicious action on your computer. One in particular that you may want to add is "\*.windowsupdate.microsoft.com" (without the quotes). This is the site that will host the update, and it requires the use of an ActiveX control to install the update.

Install the

<http://www.microsoft.com/office/previous/outlook/2002security.asp>  
Outlook E-mail Security Update if you are using Outlook 2000 SP1 or earlier:

By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been applied.

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

Install the update that is included with Microsoft Security Bulletin

<http://go.microsoft.com/fwlink/?LinkId=19527> MS04-018 if you are using Outlook Express 5.5 SP2:

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

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

Read e-mail messages in plain text format if you are using Outlook 2002 or

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

later, or Outlook Express 6 SP1 or later, to help protect yourself from the HTML e-mail attack vector:

Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or later and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only.

Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For more information about enabling this setting in Outlook 2002, see Microsoft Knowledge Base Article

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

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

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

The changes are applied to the preview pane and to open messages.

Pictures become attachments so that they are not lost.

Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.

### FAQ for CSS Heap Memory Corruption Vulnerability:

What is the scope of the vulnerability?

This is a buffer overrun vulnerability. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

What causes the vulnerability?

An unchecked buffer in Internet Explorer processing of CSS.

What are CSS?

Cascading Style Sheets (CSS) is a technology that allows Web authors to have increased control of the design and interaction of their Web pages.

For more information about CSS, visit this

<[http://msdn.microsoft.com/library/default.asp?url=/workshop/author/css/css\\_node\\_entry.asp](http://msdn.microsoft.com/library/default.asp?url=/workshop/author/css/css_node_entry.asp)> Microsoft Developer Network (MSDN) Web site.

How could an attacker exploit the vulnerability?

An attacker could exploit this vulnerability by creating a malicious Web page or an HTML e-mail message and then persuading the user to visit the page or to view the HTML e-mail message. When the user visited the page or viewed the e-mail message, the attacker could access information from other Web sites, access local files on the system, or cause malicious code to run in the security context of the locally logged on user.

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

What systems are primarily at risk from the vulnerability?

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

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

Yes. Windows 98, Windows 98 Second Edition, and Windows Millennium Edition are critically affected by this vulnerability. Critical security updates for these platforms may not be available concurrently with the other security updates that are provided as part of this security bulletin. They will be made available as soon as possible following the release. When these security updates are available, you will be able to download them only from the <<http://go.microsoft.com/fwlink/?LinkId=21130>> Windows Update Web site. For more information about severity ratings, visit this <<http://go.microsoft.com/fwlink/?LinkId=21140>> Microsoft Web site.

What does the update do?

The update removes the vulnerability by modifying the way that Internet Explorer validates the length of a message while processing CSS.

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

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CAN-2004-0842.

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

No. Microsoft had not received any information indicating 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.

Mitigating Factors for Similar Method Name Redirection Cross Domain Vulnerability:

\* 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 site.

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

\* Customers who have installed both the update referenced in Microsoft Security Bulletin <<http://go.microsoft.com/fwlink/?LinkId=30585>> MS04-024

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

and have installed the ADODB.Stream update that is referenced in Knowledge Base Article <<http://support.microsoft.com/?id=870669>> 870669 will be at a reduced risk of this vulnerability resulting in remote code execution.

\* By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the <<http://www.microsoft.com/office/outlook/evaluation/security.asp>> Outlook E-mail Security Update has been installed. Outlook Express 5.5 Service Pack 2 opens HTML e-mail in the Restricted sites zone if Microsoft Security Bulletin <<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 has been installed. The Restricted sites zone helps reduce attacks that could attempt to exploit this vulnerability.

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

\* Install the update that is included with Microsoft Security Bulletin <<http://www.microsoft.com/technet/security/bulletin/MS03-040.msp>> MS03-040 or a later Cumulative Security Update for Internet Explorer.

\* Use Outlook Express 5.5 Service Pack 2 or later and have applied the update that is included with Microsoft Security Bulletin <<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 or a later Cumulative Security Update for Outlook Express.

\* Use Microsoft Outlook 98 and Outlook 2000 with the Microsoft Outlook E-mail Security Update installed

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

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

### Workarounds for Similar Method Name Redirection Cross Domain Vulnerability:

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

Set Internet and Local Intranet security zone settings to High to prompt before running ActiveX controls and Active scripting in the Internet zone and in the Local Intranet zone:

You can help protect against these vulnerabilities by changing your settings for the Internet security zone to prompt before running ActiveX controls and Active scripting. 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 Run ActiveX controls and plug-ins in the ActiveX controls and plug-ins section, click Prompt.
5. Under Active Scripting in the Scripting section, click Prompt, and then click OK.

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

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

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

Prompting before running ActiveX controls is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you trust the site that you are visiting, click Yes to run ActiveX controls. If you do not want to be prompted for all these sites, use the "Restrict Web sites to only your trusted Web sites" workaround.

Restrict Web sites to only your trusted Web sites:

After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active scripting in the Internet zone and in the Local Intranet zone, you can add sites that you trust to Internet Explorer's Trusted sites zone. If you do this, you can 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 Internet Options on the Tools menu.
2. Click the Security tab.
3. In the Select a Web content zone to specify its current security settings box, click Trusted Sites, and then click Sites.
4. 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.
5. In the Add this Web site to the zone box, type the URL of a site that you trust, and then click Add.
6. Repeat these steps for each site that you want to add to the zone
7. Click OK two times to accept the changes and to return to Internet Explorer.

Add any sites that you trust not to take malicious action on your computer. You may want to add "\*.windowsupdate.microsoft.com" (without the quotation marks) to your Trusted Sites zone. This site hosts the update. This site uses an ActiveX control to install the update.

Strengthen the security settings for the Local Machine zone in Internet Explorer:

Because this vulnerability permits an attacker to run HTML code in the Local Machine security zone, users can reduce the impact of this

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

vulnerability by restricting the default settings in this zone. For more information about these settings, and for more information about the potential impacts of changing these default settings, see Microsoft Knowledge Base Article <<http://support.microsoft.com/?id=833633>> 833633.

Impact of Workaround: Microsoft recommends that customers consider these changes to Internet Explorer security settings as a last resort only. If you make these changes, you may lose some functionality for some Windows programs and components. Before you make these changes in a production environment, test the changes extensively to verify that mission-critical programs continue to work correctly for all users.

Install the

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

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

By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the <<http://www.microsoft.com/office/previous/outlook/2002security.asp>> Outlook E-mail Security Update has been applied.

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

Install the update that is included with Microsoft Security Bulletin MS04-018 if you are using Outlook Express 5.5 SP2:

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

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

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

Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or later and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only.

Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For more information about enabling this setting in Outlook 2002, see Microsoft Knowledge Base Article

<<http://support.microsoft.com/?id=307594>> 307594.

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

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

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

FAQ for Similar Method Name Redirection Cross Domain Vulnerability:

What is the scope of the vulnerability?

A vulnerability in the cross domain security model exists in Internet Explorer because of the way that it handles navigation methods by functions that have similar names. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could run malicious script code in the Local Machine security zone in Internet Explorer or access information in a different domain. In the worst case, if a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

What causes the vulnerability?

The process that the Internet Explorer cross-domain security model uses to validate navigation methods that have similar function names.

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

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

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

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

cross-domain security model should prevent the Web site from reading the file that is being displayed.

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

What are Internet Explorer security zones?

Internet Explorer security zones are part of a system that divides online content into categories or zones that are based on the trustworthiness of the content. Specific Web domains can be assigned to a zone, depending on how much trust is placed 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 run malicious script code in the Local Machine security zone in Internet Explorer. This could allow an attacker to take complete control of the affected system.

How could an attacker exploit the vulnerability?

An attacker could exploit this vulnerability by creating a malicious Web page or an HTML e-mail message and then convincing the user to visit this page or to view the HTML e-mail message. When the user visited the page or viewed the e-mail message, the attacker could access information from other Web sites, access local files on the system, or cause script to run in the security context of the Local Machine security zone.

What systems are primarily at risk from the vulnerability?

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

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

Yes. Windows 98, Windows 98 Second Edition, and Windows Millennium Edition are critically affected by this vulnerability. Critical security updates for these platforms may not be available concurrently with the other security updates provided as part of this security bulletin. They will be made available as soon as possible following the release. When these security updates are available, you will be able to download them only from the <<http://go.microsoft.com/fwlink/?LinkId=21130>> Windows Update Web site. For more information about severity ratings, visit this <<http://go.microsoft.com/fwlink/?LinkId=21140>> Microsoft Web site.

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

Could the vulnerability be exploited over the Internet?

Yes. An attacker may be able to exploit this vulnerability over the Internet. Microsoft has provided information on how you can help protect your PC. End users can visit the Protect Your PC Web site. IT Professionals can visit the Security Guidance Center Web site.

What does the update do?

The update removes the vulnerability by modifying the way that Internet Explorer validates navigation methods by functions that have similar names.

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

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CAN-2004-0727. It also has been named SimliarMethodNameRedir by the larger security community.

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

Yes. This security update addresses the vulnerability that is currently being exploited. The vulnerability that has been addressed has been assigned the Common Vulnerability and Exposure number CAN-2004-0727.

Mitigating Factors for Install Engine Vulnerability:

\* 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 site.

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

\* By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the Microsoft

<<http://www.microsoft.com/office/outlook/evaluation/security.asp>> Outlook E-mail Security Update has been applied. Outlook Express 5.5 Service Pack 2 opens HTML e-mail in the Restricted sites zone if the update that is included with Microsoft Security Bulletin

<<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 has been applied. The Restricted sites zone helps reduce attacks that could attempt to exploit this vulnerability.

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

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

\* Install the update that is included with Microsoft Security Bulletin <<http://www.microsoft.com/technet/security/bulletin/MS03-040.mspx>> MS03-040 or a later Cumulative Security Update for Internet Explorer.

\* Use Outlook Express 5.5 Service Pack 2 or later and have applied the update that is included with Microsoft Security Bulletin <<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 or a later Cumulative Security Update for Outlook Express.

\* Use Microsoft Outlook 98 and Outlook 2000 with the Microsoft <<http://www.microsoft.com/office/outlook/evaluation/security.asp>> Outlook E-mail Security Update applied.

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

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

### Workarounds for Install Engine Vulnerability:

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

Set Internet and Local Intranet security zone settings to High to prompt before running ActiveX controls and Active scripting in the Internet zone and in the Local Intranet zone:

You can help protect against these vulnerabilities by changing your settings for the Internet security zone to prompt before running ActiveX controls and Active scripting. 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 Run ActiveX controls and plug-ins in the ActiveX controls and plug-ins section, click Prompt.
5. Under Active Scripting in the Scripting section, click Prompt, and then click OK.
6. Click Local intranet, and then click Custom Level.
7. Under Run ActiveX controls and plug-ins in the ActiveX controls and plug-ins section, click Prompt.
8. Under Active Scripting in the Scripting section, click Prompt.
9. Click OK two times to return to Internet Explorer.

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

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

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 trust the site that you are visiting, click Yesto run ActiveX controls. If you do not want to be prompted for all these sites, use the "Restrict Web sites to only your trusted Web sites" workaround.

Restrict Web sites to only your trusted Web sites:

After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active scripting in the Internet zone and in the Local Intranet zone, you can add sites that you trust to Internet Explorer's Trusted sites zone. If you do this, you can 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 Internet Options on the Tools menu.
2. Click the Security tab.
3. In the Select a Web content zone to specify its current security settings box, click Trusted Sites, and then click Sites.
4. 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.
5. In the Add this Web site to the zone box, type the URL of a site that you trust, and then click Add.
6. Repeat these steps for each site that you want to add to the zone
7. Click OK two times to accept the changes and to return to Internet Explorer.

Add any sites that you trust not to take malicious action on your computer. You may want to add "\*.windowsupdate.microsoft.com" (without the quotation marks) to your Trusted Sites zone. This site hosts the update. This site uses an ActiveX control to install the update.

Install the

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

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

By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the

<<http://www.microsoft.com/office/outlook/evaluation/security.asp>> Outlook E-mail Security Update has been applied.

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

Install the update that is included with Microsoft Security Bulletin

<<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 if you are using Outlook Express 5.5 SP2.

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

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

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

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

Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or later and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only.

Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For more information about enabling this setting in Outlook 2002, see Microsoft Knowledge Base Article

<<http://support.microsoft.com/?id=307594>> 307594.

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

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

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

### FAQ for Install Engine Vulnerability:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. If a user is logged on with administrative privileges, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

What causes the vulnerability?

An unchecked buffer in the Internet Explorer Install Engine.

What is the Install Engine?

The Install Engine is part of the Internet Explorer Active Setup technology. Active Setup allows an installation program to receive additional files from the Internet that are needed for program initialization.

How could an attacker exploit the vulnerability?

An attacker could exploit this vulnerability by creating a malicious Web page or an HTML e-mail message and then enticing the user to visit this

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

page or to view the HTML e-mail message. When the user visited the page or viewed the e-mail message, the attacker could access information from other websites, local files on the system, or cause malicious code to run in the security context of the locally logged on user.

What systems are primarily at risk from the vulnerability?

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

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

Yes. Windows 98, Windows 98 Second Edition, and Windows Millennium Edition are critically affected by this vulnerability. Critical security updates for these platforms may not be available concurrently with the other security updates provided as part of this security bulletin. They will be made available as soon as possible following the release. When these security updates are available, you will be able to download them only from the <<http://go.microsoft.com/fwlink/?LinkId=21130>> Windows Update Web site. For more information about severity ratings, visit this <<http://go.microsoft.com/fwlink/?LinkId=21140>> Microsoft Web site.

What does the update do?

The update removes the vulnerability by modifying the way that the Install Engine in Internet Explorer validates the length of a message before it passes the message to the allocated buffer.

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 indicating 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.

Mitigating Factors for Drag and Drop Vulnerability:

\* 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 site. After they click the link, they would need to perform an action on the malicious web site that would invoke drag-and-drop handling

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

in Internet Explorer.

- \* This vulnerability allows an attacker to place malicious code on the user's system in specified locations. An attack could only occur after the user ran this code, either by restarting the system, by logging off and then logging back on to the system, or by inadvertently running the code that the attacker saved locally on the system.

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

- \* By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the <<http://www.microsoft.com/office/outlook/evaluation/security.asp>> Outlook E-mail Security Update has been applied. Outlook Express 5.5 Service Pack 2 opens HTML e-mail in the Restricted sites zone if the update that is included with Microsoft Security Bulletin

- <<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 has been applied.

The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability.

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

- \* Install the update that is included with Microsoft Security Bulletin <<http://www.microsoft.com/technet/security/bulletin/MS03-040.msp>> MS03-040 or a later Cumulative Security Update for Internet Explorer.

- \* Use Outlook Express 5.5 Service Pack 2 or later and have applied the update that is included with Microsoft Security Bulletin

- <<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 or a later Cumulative Security Update for Outlook Express.

- \* Use Microsoft Outlook 98 and Outlook 2000 with the Microsoft <<http://www.microsoft.com/office/outlook/evaluation/security.asp>> Outlook E-mail Security Update applied.

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

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

### Workarounds for Drag and Drop Vulnerability:

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

Set Internet and Local Intranet security zone settings to "High" to prompt before running ActiveX controls and Active scripting in the Internet zone and in the Local Intranet zone:

You can help protect against these vulnerabilities by changing your settings for the Internet security zone to prompt before running ActiveX controls and Active scripting. To do this, follow these steps:

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04–038)

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

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

Prompting before running ActiveX controls is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you trust the site that you are visiting, click Yes to run ActiveX controls. If you do not want to be prompted for all these sites, use the "Restrict Web sites to only your trusted Web sites" workaround.

Restrict Web sites to only your trusted Web sites:

After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active scripting in the Internet zone and in the Local Intranet zone, you can add sites that you trust to Internet Explorer's Trusted sites zone. If you do this, you can 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 Internet Options on the Tools menu.
2. Click the Security tab.
3. In the Select a Web content zone to specify its current security settings box, click Trusted Sites, and then click Sites.
4. 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.
5. In the Add this Web site to the zone box, type the URL of a site that you trust, and then click Add.
6. Repeat these steps for each site that you want to add to the zone.
7. Click OK two times to accept the changes and to return to Internet Explorer.

Add any sites that you trust not to take malicious action on your computer. You may want to add "\*.windowsupdate.microsoft.com" (without the quotation marks) to your Trusted Sites zone. This site hosts the update.

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

This site uses an ActiveX control to install the update.

Install the Outlook E-mail Security Update if you are using Outlook 2000 SP1 or earlier:

By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been applied.

Customers who use

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

Set advanced security settings to not save encrypted pages to disk:

You can help protect against these vulnerabilities by changing your settings to not save encrypted contents to disk. To do this, follow these steps:

1. In Internet Explorer, click Internet Options on the Tools menu.
2. Click the Advanced tab.
3. Under Settings, scroll to Security.
4. Under Settings, in the Security section, click Do not save encrypted pages to disk.
5. Click OK two times to return to Internet Explorer.

FAQ for SSL Caching Vulnerability:

What is the scope of the vulnerability?

This is an information disclosure and spoofing vulnerability. An attacker who successfully exploited this vulnerability could gain access to information or spoof content on SSL protected Web sites.

What causes the vulnerability?

Internet Explorer's handling of cached SSL contents.

What is SSL?

<<http://www.ietf.org/rfc/rfc2246.txt>> Secure Sockets Layer (SSL) is a protocol that allows web sessions to be encrypted for greater security. In Internet Explorer, when you visit a Web site and a yellow lock icon appears in the lower right corner of the browser window, the current session is protected by SSL.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could access information or spoof content on Web sites that are protected by SSL.

How could an attacker exploit the vulnerability?

An attacker could exploit the vulnerability by creating a Web site that has the same host name as a legitimate SSL protected Web site. If the attacker were then able to redirect navigation from the legitimate Web Site at that address to their malicious Web site, items of the attacker's choosing could be cached to the local system.

When the user visited the legitimate site in a second session, these items

## Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-038)

would be loaded in the context of the legitimate Web site. These items could include script code, images, or other locally cached content. This content could be crafted to obtain sensitive information that would typically be protected by SSL security.

What systems are primarily at risk from the vulnerability?

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

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

No. Although Windows 98, Windows 98 Second Edition, and Windows Millennium Edition do contain the affected component, the vulnerability is not critical. For more information about severity ratings, visit this <http://go.microsoft.com/fwlink/?LinkId=21140> Microsoft Web site.

What does the update do?

The update removes the vulnerability by modifying the way that Internet Explorer validates content during SSL sessions.

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

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

### ADDITIONAL INFORMATION

The information has been provided by Micros