

[NT] Cumulative Security Update for Internet Explorer (MS04-025)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0011.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/03/04

To: list@securiteam.com

Date: 3 Aug 2004 17:21:35 +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 (MS04-025)

SUMMARY

The cumulative update for Internet Explorer resolves three new vulnerabilities, all of which enable an attacker to execute arbitrary code on a target system. The first vulnerability deals with cross-domain attacks while the other two are caused by mishandling of the BMP and GIF file formats.

DETAILS

Affected Software:

- * Microsoft Windows NT Workstation 4.0 Service Pack 6a
- * 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 2, Microsoft Windows 2000 Service Pack 3, Microsoft Windows 2000 Service Pack 4
- * Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- * Microsoft Windows XP 64-Bit Edition Service Pack 1
- * Microsoft Windows XP 64-Bit Edition Version 2003
- * Microsoft Windows Server 2003
- * Microsoft Windows Server 2003 64-Bit Edition

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-025)

* 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 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=507E71EF-076B-43C4-8028-E91FCFAB252B&dis>

Download the update

* Internet Explorer 5.01 Service Pack 3 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7AA6F31D-7350-43F8-B72E-ED9D62577A60&dis>

Download the update

* Internet Explorer 5.01 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=862E6914-821A-4C51-985B-C3958FAD3D4C&dis>

Download the update

* Internet Explorer 5.5 Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E458480C-93F6-454A-A663-FC187C18CD9B&dis>

Download the update

* Internet Explorer 6 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4C2F8A40-1B88-4F93-98B1-1619DCFD7273&dis>

Download the update

* Internet Explorer 6 Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=06F49985-F19F-4B50-A75F-7636D8BEE576&dis>

Download the update

* Internet Explorer 6 Service Pack 1 (64-Bit Edition) –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=FCDA580D-9E3B-4B44-BD65-C8D37A0DD62D&dis>

Download the update

* Internet Explorer 6 for Windows Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=D86262D9-C66A-4608-8DBE-2492B4AFBC3B&dis>

Download the update

* Internet Explorer 6 for Windows Server 2003 (64-Bit Edition) –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1AA8F5A9-71D3-48F7-BB32-F8A4D36C5FB9&dis>

Download the update

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0549>>

CAN-2004-0549

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0566>>

CAN-2004-0566

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1048>>

CAN-2003-1048

Navigation Method Cross-Domain Vulnerability

A remote code execution vulnerability exists in Internet Explorer because of the way that it handles navigation methods. 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. If a user is logged on with administrative privileges, this could allow the attacker to take complete control of an affected system.

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-025)

Mitigating Factors for Navigation Method 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 and have installed the ADODB.Stream update that is referenced in Knowledge Base Article <<http://support.microsoft.com/default.aspx?kbid=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:

* Apply 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 vulnerability for more information about Internet Explorer Enhanced Security Configuration.

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-025)

Workarounds for Navigation Method Cross-Domain Vulnerability

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

- * In Internet Explorer, click Internet Options on the Tools menu.
- * Click the Security tab.
- * Click Internet, and click Custom Level.
- * Under Settings, in the ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt.
- * In the Scripting section, under Active Scripting, click Prompt, and then click OK.
- * Click Local intranet, and then click Custom Level.
- * Under Settings, in the ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt.
- * In the Scripting section, under Active Scripting, click Prompt.
- * Click OK two times to return to Internet Explorer.

Impact of wordaround: 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. 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.

* 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:

- * In Internet Explorer, click Tools, click Internet Options, and then click the Security tab.
- * In the Select a Web content zone to specify its current security settings box, click Trusted Sites, and then click Sites.
- * 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.
- * In the Add this Web site to the zone box, type the URL of a site that you trust, and then click Add.
- * Repeat these steps for each site that you want to add to the zone.
- * Click OK two times to accept the changes and return to Internet Explorer.

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-025)

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.

* 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 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/default.aspx?scid=kb:EN-US:833633>> 833633.

Impact of Workaround: If you make these changes, you may lose some functionality for some Windows programs and components.

* Install Outlook

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

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

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

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

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

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.

Malformed BMP File Buffer Overrun Vulnerability

A buffer overrun vulnerability exists in the processing of BMP image file formats that could allow remote code execution on an affected system. If the user is logged on with administrative privileges an attacker who successfully exploited this vulnerability could take complete control of the 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.

Mitigating Factors for Malformed BMP File Buffer Overrun 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.

Workarounds for Malformed BMP File Buffer Overrun Vulnerability

* 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/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.

Malformed GIF File Double Free Vulnerability

A buffer overrun vulnerability exists in the processing of GIF image file formats that could allow remote code execution on an affected system. If the user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of the 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.

Mitigating Factors for Malformed GIF File Double Free 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.

* Because of the unique layout of the memory structures on each affected system, exploiting this vulnerability on a mass scale could potentially be difficult.

Workarounds for Malformed GIF File Double Free Vulnerability

The same workaround present for the BMP buffer overrun can be used for this vulnerability. See the above section for more details.

Frequently asked questions (FAQ) related to this security update

Why is this update being re-released ?

Subsequent to the release of MS04-025, Microsoft was made aware that the update provided for Windows XP customers running the new version of Windows Update, Windows Update Version 5, did not contain the proper fixes for the vulnerabilities discussed in the security bulletin. Microsoft has corrected the update and is re-releasing the bulletin to advise of the availability of the revised update. Customers who are running Windows Update Version 5 who have automatic updates enabled need take no action, as the revised update will be delivered automatically. Customers who manually utilize Windows Update and are running Windows Update Version 5 need to revisit the Windows Update site and download the revised update at <http://windowsupdate.microsoft.com>.

How do I know if I m running Windows Update Version 5 ?

Customers can verify if they are using Windows Update Version 5 by looking for the Express Install arrow on the Windows Update home page. If you see the Express Install arrow on the home page you have version 5 installed. If you see the Express Install arrow, click on the link and the new

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-025)

update will be offered to you. If you do not have an Express Install link in the Windows Update page, then you are not running version 5 and are not affected.

What is Windows Update Version 5 ?

Windows Update Version 5 is the newest version of the Windows Update service that began rolling out to customers this week. There are several enhancements in Windows Update Version 5 that will not only help users keep their PCs secure but will improve ease of use and discoverability of the site. The site now offers two easy-to-use installation options Express and Custom — to quickly find the updates that best meet a customer's need. WU and AU are now both optimized for dial up and low bandwidth users. For instance, if a customer loses Internet connectivity, the download will pick up where it left off in the last download session. A new homepage design and navigation taxonomy also make Windows Update easier to navigate and provide better integration with related customer offerings such as Automatic Update.

I'm not on Windows Update Version 5. How do I get it ?

If you're on Windows XP and have Automatic Updates turned on, you will receive Windows Update Version 5 automatically in the next few weeks. If you don't have Automatic Updates turned on, you will be upgraded to Windows Update Version 5 when you visit the Windows Update site after the initial rollout to users with Automatic Updates is complete. This is expected to take another few weeks.

I use Software Update Services (SUS) to deploy my security updates. Do I need to re-deploy this update ?

No. While SUS does leverage Windows Update technology to help deploy security updates, SUS does not use Windows Update Version 5 and is not impacted by this re-release.

I use Systems Management Services (SMS) to deploy my security updates. Do I need to re-deploy this update ?

No. This problem specifically affects Windows Update Version 5 and does not affect customers using SMS at all.

Why does this update address several reported security vulnerabilities ?

This update contains support for several vulnerabilities because the modifications that are required to address these issues are located in related files. Instead of having to install several updates that are almost the same, customers can install only this update.

What updates does this release replace ?

This is a cumulative update that includes the functionality of all the previously released updates for Internet Explorer.

I've received a hotfix from Microsoft or my support provider since the release of <http://support.microsoft.com/?kbid=824684> MS04-004. Is that hotfix included in this Security Update ?

No. For all operating systems besides Microsoft Windows Server 2003 or

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-025)

Microsoft Windows 64-Bit Edition Version 2003, most hotfixes created after MS04-004 are not included in this security update. Installing this security update will remove these hotfixes from the system. An <http://support.microsoft.com/?kbid=824684> update rollup is available that contains these hotfixes as well as fixes for all the security issues addressed in this update. For more information on what hotfixes are not included in this security update but that are included in the update rollup, as well as instructions on how to obtain and deploy the update rollup, contact your Microsoft support provider or review Microsoft Knowledge Base Article <http://support.microsoft.com/?kbid=871260> 871260.

I've installed a publicly available Update for Internet Explorer since the release of MS04-004. Is this update included in this Security Update ? Yes, the publicly available updates for Internet Explorer released since MS04-004 are included in this security update. This includes the following updates:

- * The update for Internet Explorer 6 Service Pack 1 provided with Microsoft Knowledge Base Article <http://support.microsoft.com/?kbid=831167> 831167 entitled "You cannot log on to a Web site or complete an Internet transaction, or you receive an HTTP 500 (Internal Server Error) Web page"

- * The update for Internet Explorer 5.5 Service Pack 2 provided with Microsoft Knowledge Base Article <http://support.microsoft.com/?kbid=837209> 837209 entitled An HTTPS Web page does not download completely in Internet Explorer 5.5

- * The update for Internet Explorer 6 for Windows Server 2003 provided with Microsoft Knowledge Base Article <http://support.microsoft.com/?kbid=839571> 839571 entitled "Connections do not use LAN automatic configuration and proxy settings in Windows Server 2003"

- * The update for Internet Explorer 6 for Windows Server 2003 provided with Microsoft Knowledge Base Article <http://support.microsoft.com/?kbid=817786> 817786 entitled "An Access Violation Occurs When You Refresh a Web Page in Internet Explorer"

I m running Windows XP Service Pack 1 and have received the hotfix associated with Microsoft Knowledge Base Article 840309 from my Premier Support professional. What should I do before I apply this update ? Customers who have installed this hotfix may experience problems with their desktop startup after installing this update. Microsoft Knowledge Base Article <http://support.microsoft.com/?kbid=840309> 840309 has been updated with workarounds to avoid these symptoms.

Does this update contain any other security changes ?

Yes. This update contains two additional security changes. The update refines a change made in Internet Explorer 6 Service Pack 1, which prevents web pages in the Internet zone from navigating to the Local Machine zone. This change was introduced to mitigate the effects of potential new cross domain vulnerabilities. The changes introduced in this update are further enhancements of the Internet Explorer 6 Service Pack 1

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-025)

restrictions. The update also further enforces the cross domain security model in Internet Explorer. This change is further documented in Microsoft Knowledge Base Article <<http://support.microsoft.com/?kbid=875345>> 875345.

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

Microsoft will only release security updates for critical security issues. Non-critical security issues are not offered during this support period. For more information about the Microsoft Support Lifecycle policies for these operating systems, visit the following <<http://support.microsoft.com/default.aspx?pr=LifeAn1>> Web site.

For more information about severity ratings, visit the following <<http://go.microsoft.com/fwlink/?LinkId=21140>> Web site.

Are Windows 98, Windows 98 Second Edition, or Windows Millennium Edition critically affected by any of the vulnerabilities that are addressed in this security bulletin ?

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 the following <<http://go.microsoft.com/fwlink/?LinkId=21140>> Web site.

I'm still using Microsoft Windows NT 4.0 Workstation Service Pack 6a or Windows 2000 Service Pack 2, but extended security update support ended on June 30, 2004. However, this bulletin has a security update for these operating system versions. Why is that ?

Windows NT 4.0 Workstation Service Pack 6a and Windows 2000 Service Pack 2 have reached the end of their life cycles as previously documented, and Microsoft extended this support to June 30, 2004. However, the end-of-life for the extended support period occurred very recently. In this case, the majority of the steps that are required to address this vulnerability were completed before June 30, 2004. Therefore, we have decided to release security updates for these operating system versions as part of this security bulletin. We do not anticipate doing this for future vulnerabilities affecting these operating system versions, but we reserve the right to produce updates and to make these updates available when necessary.

It should be a priority for customers who have these operating system versions to migrate to supported versions to prevent potential exposure to future vulnerabilities. For more information about the Windows Product Life Cycle, visit the following

<<http://go.microsoft.com/fwlink/?LinkId=21742>> Microsoft Support Lifecycle

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-025)

Web site. For more information about the extended security update support period for these operating system versions, visit the following <http://support.microsoft.com/default.aspx?scid=fh:5bLN%5d:LifeAnOct2003> Microsoft Product Support Services Web site.

Customers who require additional support for Windows NT Workstation 4.0 SP6a must contact their Microsoft account team representative, their Technical Account Manager, or the appropriate Microsoft partner representative for custom support options. Customers without an Alliance, Premier, or Authorized Contract can contact their local Microsoft sales office. For contact information, visit the <http://www.microsoft.com/worldwide/> Microsoft Worldwide Information Web site, select the country, and then click Go to see a list of phone numbers. When you call, ask to speak with the local Premier Support sales manager.

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

Yes. MBSA will determine if this update is required. For more information about MBSA, visit the <http://go.microsoft.com/fwlink/?LinkId=21134> MBSA Web site.

Note: After April 20, 2004, the Mssecure.xml file that is used by MBSA 1.1.1 and earlier versions is no longer being updated with new security bulletin data. Therefore, scans that are performed after that date with MBSA 1.1.1 or earlier will be incomplete. All users should upgrade to MBSA 1.2 because it provides more accurate security update detection and supports additional products. Users can download MBSA 1.2 from the MBSA Web site. For more information about MBSA support, visit the following Microsoft Baseline Security Analyzer 1.2 Q&A Web site.

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

Yes. SMS can help detect and deploy this security update. For information about SMS, visit the <http://go.microsoft.com/fwlink/?LinkId=21158> SMS Web site.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security. The original article can be found at: <http://www.microsoft.com/technet/security/bulletin/ms04-025.mspx> <http://www.microsoft.com/technet/security/bulletin/ms04-025.mspx>

=====

This bulletin is sent to members of the SecuriTeam mailing list. To unsubscribe from the list, send mail with an empty subject line and body to: list-unsubscribe@securiteam.com In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS04-025)

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.