

# [NT] Cumulative Security Update for Internet Explorer (MS08-024)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-04/msg00026.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 9 Apr 2008 16:20:12 +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 (MS08-024)

---

## SUMMARY

This security update resolves one privately reported vulnerability. The vulnerability could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer. 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 security update is rated Critical for all supported releases of Internet Explorer. For more information, see the subsection, Affected and Non-Affected Software, in this section.

## DETAILS

Affected Software:

Operating System – Component – Maximum Security Impact – Aggregate Severity Rating – Bulletins Replaced by This Update

Internet Explorer 5.01 and Internet Explorer 6 Service Pack 1

\* Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B051AE04-FE81-440D-9136-D6B239CA954E>>

Microsoft Internet Explorer 5.01 Service Pack 4 – Remote Code Execution – Critical – MS08-010

## [NT] Cumulative Security Update for Internet Explorer (MS08-024)

\* Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=75D2DC78-E3A4-4FF6-9E2D-BF1935003E8E>>

Microsoft Internet Explorer 6 Service Pack 1 – Remote Code Execution – Critical – MS08-010

### Internet Explorer 6

\* Windows XP Service Pack 2 – Microsoft Internet Explorer 6 – Remote Code Execution – Critical – MS08-010

\* Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=36C641AD-953F-4B09-BA1C-9C383295E180>>

Microsoft Internet Explorer 6 – Remote Code Execution – Critical – MS08-010

\* Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=85BEACC0-8CA2-4DED-9C24-23348D05C735>>

Microsoft Internet Explorer 6 – Remote Code Execution – Critical – MS08-010

\* Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=5EBB5EF9-615F-4CAB-BAC5-6F45F1B94952>>

Microsoft Internet Explorer 6 – Remote Code Execution – Critical – MS08-010

\* Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=63DA8040-FDA2-42C7-8543-26AD6F9811F2>>

Microsoft Internet Explorer 6 – Remote Code Execution – Critical – MS08-010

### Internet Explorer 7

\* Windows XP Service Pack 2 – Windows Internet Explorer 7 – Remote Code Execution – Critical – MS08-010

\* Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E771EFE8-8881-4F23-B5B0-15651A390BA9>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS08-010

\* Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9364BF81-6505-4788-958D-A4BD29DC98AD>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS08-010

\* Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9ACD2A03-5530-49C8-9EA1-0BFAF259700D>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS08-010

\* Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A9E406AA-33E2-49B8-AB54-4A7328E46147>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS08-010

\* Windows Vista and Windows Vista Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=75A05D3A-92A0-4A00-95D4-E2B2F6755180>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS08-010

\* Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=D4E24966-6530-463A-9EE2-F6A9D000F998>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – MS08-010

\* Windows Server 2008 for 32-bit Systems –

## [NT] Cumulative Security Update for Internet Explorer (MS08-024)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=295CF8F2-265E-4570-B708-21033337FE05>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – Not Applicable

\* Windows Server 2008 for x64-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E57B4D94-19AD-4818-8311-A3F94BE01A4B>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – Not Applicable

\* Windows Server 2008 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=93E9F52A-C7D0-4033-9C12-740665A219AF>>

Windows Internet Explorer 7 – Remote Code Execution – Critical – Not Applicable

### Data Stream Handling Memory Corruption Vulnerability – CVE-2008-1085

A remote code execution vulnerability exists in Internet Explorer because of the way that it processes data streams. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

#### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1085>>

CVE-2008-1085

### Mitigating Factors for Data Stream Handling Memory Corruption Vulnerability – CVE-2008-1085

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

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

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

Note It cannot be ruled out that this vulnerability could be used in an exploit without Active Scripting. However, using Active Scripting significantly increases the chances of a successful exploit. As a result, this vulnerability has been given a severity rating of Critical on Windows Server 2003 and Windows Server 2008.

### Workarounds for Data Stream Handling Memory Corruption Vulnerability – CVE-2008-1085

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- \* Read e-mail messages in plain text format to help protect yourself from the HTML e-mail attack vector

You can help protect yourself against this vulnerability by changing your e-mail settings to read e-mail messages in plain text using Outlook 2002 and later, Outlook Express 6 and later, or Windows Mail. For information in Outlook, search plain text in Help and review Read messages in plain text. In Outlook Express, search plain text in Help and review Reducing your risk of getting e-mail viruses. In Windows Mail, search plain text in Help and review Security and privacy in Windows Mail.

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

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

- \* Pictures become attachments so that they are not lost.

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

### FAQ for Data Stream Handling Memory Corruption Vulnerability – CVE-2008-1085

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

What causes the vulnerability?

When Internet Explorer processes specially crafted data streams, Internet Explorer may corrupt system memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?

## [NT] Cumulative Security Update for Internet Explorer (MS08-024)

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

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user be logged on and visit 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.

What does the update do?

The update removes the vulnerability by modifying the way that Internet Explorer processes data streams.

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.

### 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/MS08-024.msp>>  
<http://www.microsoft.com/technet/security/Bulletin/MS08-024.msp>

[NT] Cumulative Security Update for Internet Explorer (MS08-024)

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

**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.