

# [NT] Microsoft JScript Remote Code Execution (MS06-023)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-06/msg00044.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 14 Jun 2006 12:26:20 +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>

-----

Microsoft JScript Remote Code Execution (MS06-023)

---

## SUMMARY

There is a remote code execution vulnerability in JScript. An attacker could exploit the vulnerability by constructing specially crafted JScript that could potentially allow remote code execution if a user visited a Web site or viewed a specially crafted e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

A vulnerability in Microsoft JScript could allow remote code execution.

## DETAILS

### Vulnerable Systems:

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

## [NT] Microsoft JScript Remote Code Execution (MS06-023)

Windows Server 2003 with SP1 for Itanium-based Systems

- \* Microsoft Windows Server 2003 x64 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:

- \* Microsoft JScript 5.1 on Microsoft Windows 2000 Service Pack 4 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=23E79ABD-B1FE-4734-B3D3-FB53D286C06F>>

Download the update

- \* Microsoft JScript 5.6 and 5.5 when installed on Windows 2000 Service Pack 4 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=16DD21A1-C4EE-4ECA-8B80-7BD1DFEFB4F8>>

Download the update

- \* Microsoft JScript 5.6 on Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=D28C02BE-CAC3-4579-9B93-939FD5D3CDE6>>

Download the update

- \* Microsoft JScript 5.6 on Microsoft Windows XP Professional x64 Edition

–

<http://www.microsoft.com/downloads/details.aspx?FamilyId=2EE3DD28-7167-4A2C-941D-A236F8CC5C4B>>

Download the update

- \* Microsoft JScript 5.6 on Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=8963AE25-2230-47FE-AECE-49D7457D96D4>>

Download the update

- \* Microsoft JScript 5.6 on Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=7764C7DC-A7E4-4B91-95C2-EF7D4DCE0A00>>

Download the update

- \* Microsoft JScript 5.6 on Microsoft Windows Server 2003 x64 Edition –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=BCF7AB2E-EE1C-45F9-8B1C-4B1CEF683082>>

Download the update

- \* Microsoft JScript 5.6 on Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me)

Note:

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

Mitigating Factors for Microsoft JScript Memory Corruption Vulnerability:

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

## [NT] Microsoft JScript Remote Code Execution (MS06-023)

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.

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

\* By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally Outlook 2000 opens HTML e-mail messages in the Restricted sites zone if the <http://go.microsoft.com/fwlink/?LinkId=33334> Outlook E-mail Security Update has been installed. Outlook Express 5.5 Service Pack 2 opens HTML e-mail messages in the Restricted sites zone if Microsoft Security Bulletin <http://go.microsoft.com/fwlink/?LinkId=19527> MS04-018 has been installed.

\* By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as [http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc\\_changes.asp](http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc_changes.asp) Enhanced Security Configuration. This mode mitigates this vulnerability. See the FAQ section of this security update for more information about Internet Explorer Enhanced Security Configuration.

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

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

You can help protect against this vulnerability by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, follow these steps:

1. In Internet Explorer, click Internet Options on the Tools menu.
2. Click the Security tab.
3. Click Internet, and then click Custom Level.
4. Under Settings, in the Scripting section, under Active Scripting, click Prompt or Disable, and then click OK.

5. Click Local intranet, and then click Custom Level.
6. Under Settings, in the Scripting section, under Active Scripting, click Prompt or Disable, and then click OK.
7. Click OK two times to return to Internet Explorer.

Note Disabling Active Scripting in the Internet and Local intranet security zones may cause some Web sites to work incorrectly. If you have difficulty using a Web site after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly.

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

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

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

To do this, follow these steps:

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

6. Click OK two times to accept the changes and return to Internet Explorer.

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

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

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

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

1. On the Internet Explorer Tools menu, click Internet Options.
2. In the Internet Options dialog box, click the Security tab, and then click the Internet icon.
3. Under Security level for this zone, move the slider to High. This sets the security level for all Web sites you visit to High.

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

Note Setting the level to High may cause some Web sites to work incorrectly. If you have difficulty using a Web site after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High.

Impact of Workaround: There are side effects to prompting before running ActiveX Controls and Active Scripting. Many Web sites that are on the Internet or on an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or account statements. Prompting before running ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click Yes to run ActiveX Controls or Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that you trust to Internet Explorer's Trusted sites zone."

## [NT] Microsoft JScript Remote Code Execution (MS06-023)

\* Add sites that you trust to Internet Explorer's Trusted sites zone.

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

To do this, follow these steps:

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

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

\* Modify the Access Control List on JScript.dll to temporarily prevent it from running in Internet Explorer

To modify the Access Control List (ACL) on the JScript.dll file to be more restrictive, follow these steps:

1. Click Start, click Run, type `"cmd"` (without the quotation marks), and then click OK.
2. Type the following commands at a command prompt. Make a note of the current files ACLs, including inheritance settings. You may need this list if you have to undo these modifications:  
`cacls %windir%\system32\jscript.dll`
3. Type the following command at a command prompt to deny the everyone

## [NT] Microsoft JScript Remote Code Execution (MS06-023)

group access to this file:

```
echo y|cacls %windir%\system32\jscript.dll /d everyone
```

4. Close Internet Explorer, and reopen it for the changes to take effect.

Impact of Workaround: Applications and Web sites that use JScript may no longer work.

To regain functionality you must undo the modifications to the Access Control List on the jscript.dll file.

FAQ for Microsoft JScript Memory Corruption Vulnerability:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. 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?

Microsoft JScript may release objects early potentially causing memory corruption.

What is Microsoft JScript?

JScript is the Microsoft implementation of the ECMA 262 language specification (ECMAScript Edition 3). JScript is an interpreted, object-based scripting language. For more information see the <http://msdn.microsoft.com/library/en-us/dnanchor/html/scriptinga.asp> product documentation.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system.

How could an attacker exploit the vulnerability?

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

## [NT] Microsoft JScript Remote Code Execution (MS06-023)

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers could be at more risk if users who do not have sufficient administrative permissions are given the ability to log on to servers and to run programs. However, best practices strongly discourage allowing this.

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 the vulnerabilities that are addressed in this security bulletin. Critical security updates for these platforms are available, are provided as part of this security bulletin, and can be downloaded only from the <http://update.microsoft.com/microsoftupdate/> Microsoft Update Web site or from the <http://go.microsoft.com/fwlink/?LinkId=21130> Windows Update Web site. For more information about severity ratings, visit the following <http://go.microsoft.com/fwlink/?LinkId=21140> Web site.

What does the update do?

The update removes the vulnerability by guarding objects in use by JScript from early release.

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

No. Microsoft is releasing this update as a companion to the update included with <http://go.microsoft.com/fwlink/?LinkId=66973> Microsoft Security Bulletin MS06-021: Cumulative Security Update for Internet Explorer (916281). It is recommended that this update is installed at the same time as that update as a security update in that bulletin could expose this vulnerability or cause application compatibility issues.

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.

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1313>  
CVE-2006-1313

### ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

The original article can be found at:

<http://www.microsoft.com/technet/security/bulletin/ms06-023.mspx>  
<http://www.microsoft.com/technet/security/bulletin/ms06-023.mspx>

[NT] Microsoft JScript Remote Code Execution (MS06-023)

=====

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.