

# [NT] Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS07-042)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-08/msg00013.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 15 Aug 2007 16:13:05 +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>

-----

Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS07-042)

---

## SUMMARY

A remote code execution vulnerability exists in Microsoft XML Core Services that could allow an attacker who successfully exploited this vulnerability to make changes to the system with the permissions of the logged-on user. If a user is logged on with administrative user rights, an attacker could take complete control of the 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.

## DETAILS

Affected Software:

- \* Windows 2000 Service Pack 4
- \* Windows XP Service Pack 2
- \* Windows XP Professional x64 Edition
- \* Windows XP Professional x64 Edition Service Pack 2
- \* Windows Server 2003 Service Pack 1

## [NT] Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS07-042)

- \* Windows Server 2003 Service Pack 2
- \* Windows Server 2003 x64 Edition
- \* Windows Server 2003 x64 Edition Service Pack 2
- \* Windows Server 2003 with SP1 for Itanium-based Systems
- \* Windows Server 2003 with SP2 for Itanium-based Systems
- \* Windows Vista
- \* Windows Vista x64 Edition
- \* Microsoft Office 2003 Service Pack 2
- \* 2007 Microsoft Office System
- \* Microsoft Office SharePoint Server
- \* Microsoft Office Groove Server 2007

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2223>>  
CVE-2007-2223

### Mitigating Factors for Microsoft XML Core Services Vulnerability:

- \* Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:
  - \* 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, Web sites that accept or host user-provided content, or compromised Web sites and advertisement servers could contain specially crafted content that could exploit this vulnerability. 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 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 versions 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.
  - \* By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that have not been added to Internet Explorer Trusted sites zone. See the FAQ subsection of this vulnerability section for more information about Internet Explorer Enhanced Security Configuration.

## [NT] Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS07-042)

#### Workarounds for Microsoft XML Core Services Vulnerability:

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:

\* 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.

Impact of Workaround: 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..

\* Add sites that you trust to the Internet Explorer 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 the Internet Explorer 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.

## [NT] Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS07-042)

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 system. Two in particular that you may want to add are "\*.windowsupdate.microsoft.com" and \*.update.microsoft.com (without the quotation marks). These are the sites that will host the update, and it requires an ActiveX Control to install the update.

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

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

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

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

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

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

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

FAQ for Microsoft XML Core Services Vulnerability:

What is the scope of the vulnerability?

If successfully exploited, this remote code execution vulnerability could allow the attacker to run arbitrary code as the logged on user.

What causes the vulnerability?

## [NT] Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS07-042)

Specially crafted script requests may cause memory corruption when using Microsoft XML Core Services.

What is Microsoft XML Core Services (MSXML)?

Microsoft XML Core Services (MSXML) allows customers who use JScript, Visual Basic Scripting Edition (VBScript), and Microsoft Visual Studio 6.0 to develop XML-based applications that provide interoperability with other applications that adhere to the XML 1.0 standard. See the MSDN Web site for more information regarding MSXML.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could make changes to the system with the permissions of the logged-on user. If a user is logged on with administrative user rights, an attacker could take complete control of the 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.

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 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 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 request that takes users to the attacker's Web site. It could also be possible to display specially crafted Web content by using banner advertisements or by using other methods to deliver Web content to affected systems.

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user is logged on and visits 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.

I am running Internet Explorer on Windows Server 2003. Does this mitigate this vulnerability?

Yes. By default, Internet Explorer for Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. Enhanced Security Configuration is a group of preconfigured settings in Internet Explorer that can reduce the likelihood of a user or administrator downloading and running malicious Web content on a server. This is a mitigating factor for Web sites that you have not added to the Internet Explorer Trusted sites zone. See also Managing Internet Explorer Enhanced Security Configuration.

[NT] Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (MS07-042)

What does the update do?

The update removes the vulnerability by validating the memory request within Microsoft XML Core Services.

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

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

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 Security Bulletin MS07-042.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS07-042.mspx>>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-042.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@xxxxxxxxxxxxxx

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

=====  
=====

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.