

[NT] Microsoft Agent Remote Code Execution (MS07-020)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00027.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 17 Apr 2007 19:27:39 +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 Agent Remote Code Execution (MS07-020)

SUMMARY

A remote code execution vulnerability exists in Microsoft Agent in the way that it handles certain specially crafted URLs.

DETAILS

Affected Software:

- * Microsoft Windows 2000 Service Pack 4 –
<<http://www.microsoft.com/downloads/details.aspx?FamilyId=49dc470b-64e2-47ec-be90-622b407c7751>>
Download the update
- * Microsoft Windows XP Service Pack 2 –
<<http://www.microsoft.com/downloads/details.aspx?FamilyId=e16deda-6e8c-40d6-a3c0-d61362411acc>>
Download the update
- * Microsoft Windows XP Professional x64 Edition and Microsoft Windows XP Professional x64 Edition Service Pack 2 –
<<http://www.microsoft.com/downloads/details.aspx?FamilyId=23909036-898f-41af-a3de-4a899a15d25d>>
Download the update
- * Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 and Microsoft Server 2003 Service Pack 2 –
<<http://www.microsoft.com/downloads/details.aspx?FamilyId=281f10d2-d754-44cd-8318-9ce94b8d01b4>>

[NT] Microsoft Agent Remote Code Execution (MS07-020)

Download the update

* Microsoft Windows Server 2003 x64 Edition with Service Pack 1 and Microsoft Windows Server 2003 x64 Edition with Service Pack 2 – <http://www.microsoft.com/downloads/details.aspx?FamilyId=50469b54-b6ff-46ed-b2bc-3b00b0984e1e>

Download the update

* Microsoft Windows Server 2003 for Itanium-based Systems, Microsoft Windows Server 2003 with SP1 for Itanium-based Systems, and Microsoft Windows Server 2003 with SP2 for Itanium-based Systems – <http://www.microsoft.com/downloads/details.aspx?FamilyId=883660ca-e976-460f-8e50-c19d1b02b42f>

Download the update

Non-Affected Software:

- * Windows Vista
- * Windows Vista x64 Edition

Mitigating Factors for Microsoft Agent URL Parsing Vulnerability – CVE-2007-1205:

- * 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 specially crafted Web site. Instead, an attacker would have to convince them to visit the Web site, typically by getting them to click a link that takes them 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 attacks that could try to 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.
- * Internet Explorer 7 contains code changes that help prevent attempts to exploit this vulnerability. While the vulnerability in Microsoft Agent exists on supported versions of the Windows platforms, Internet Explorer 7 blocks the attack vector into the vulnerability when installed on supported platforms.

[NT] Microsoft Agent Remote Code Execution (MS07-020)

* Windows Vista is not affected by this vulnerability.

Workarounds for Microsoft Agent URL Parsing Vulnerability – CVE-2007-1205:

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.

* Temporarily prevent the Agent ActiveX control from running in Internet Explorer.

You can help prevent attempts to instantiate this ActiveX control in Internet Explorer by setting the kill bit for the control in the registry.

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use the Registry Editor at your own risk.

For detailed steps that you can use to prevent a control from running in Internet Explorer, see Microsoft Knowledge Base Article 240797. Follow these steps in this article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer.

To set the kill bit for a CLSID with a value of {D45FD31B-5C6E-11D1-9EC1-00C04FD7081F}, paste the following text in a text editor such as Notepad. Then, save the file by using the .reg file name extension.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX  
Compatibility\{D45FD31B-5C6E-11D1-9EC1-00C04FD7081F}]
```

```
"Compatibility Flags"=dword:00000400
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX  
Compatibility\{F5BE8BD2-7DE6-11D0-91FE-00C04FD701A5}]
```

```
"Compatibility Flags"=dword:00000400
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX  
Compatibility\{4BAC124B-78C8-11D1-B9A8-00C04FD97575}]
```

```
"Compatibility Flags"=dword:00000400
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX  
Compatibility\{D45FD31D-5C6E-11D1-9EC1-00C04FD7081F}]
```

```
"Compatibility Flags"=dword:00000400
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX  
Compatibility\{D45FD31E-5C6E-11D1-9EC1-00C04FD7081F}]
```

[NT] Microsoft Agent Remote Code Execution (MS07-020)

"Compatibility Flags"=dword:00000400

You can apply this .reg file to individual systems by double-clicking it.

You can also apply it across domains by using Group Policy. For more information about Group Policy, visit the following Microsoft Web sites:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/6d7cb788-b31d-4d17-9f1e-b5>
Group Policy collection

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/47ba1311-6cca-414f-98c9-2d>
What is Group Policy Object Editor?

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/e926577a-5619-4912-b5d9-e7>
Core Group Policy tools and settings

Note You must restart Internet Explorer for your changes to take effect.

Impact of workaround: Web sites that use the Microsoft Agent ActiveX Control will no longer work correctly via Internet Explorer.

* Unregister AgentSvr.exe

Type the following at a command line or in a logon / machine startup script:

```
%windir%\msagent\agentsvr.exe /unregserver
```

Impact of workaround: The Microsoft Agent will no longer work.

* Configure Internet Explorer to prompt before running ActiveX Controls or disable ActiveX Controls in the Internet and Local intranet security zone.

You can help protect against this vulnerability by changing your Internet Explorer settings to prompt before running ActiveX controls. 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 ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt or Disable, and then click OK.
5. Click Local intranet, and then click Custom Level.
6. Under Settings, in the ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt or Disable, and then click OK.
7. 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 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 .

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.
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. 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 .

* 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.

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.

FAQ for Microsoft Agent URL Parsing Vulnerability – CVE-2007-1205:

What is the scope of the vulnerability?

A remote code execution vulnerability exists in Microsoft Agent in the way that it handles certain specially crafted URLs. 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.

What causes the vulnerability?

A specially crafted URL could corrupt system memory in such a way that an attacker could execute arbitrary code when supplied to Microsoft Agent control.

What is Microsoft Agent?

Microsoft Agent is a component that uses interactive animated characters to guide users and can make using and learning to use a computer easier. For more information, see the Microsoft Agent Web site.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability 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.

Who could exploit the 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 attempt to exploit this vulnerability. An attacker would have no way to force users to visit a specially crafted Web site. Instead, an attacker would have to convince them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site.

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.

[NT] Microsoft Agent Remote Code Execution (MS07-020)

I am running Windows Internet Explorer 7. Does this mitigate this vulnerability?

Yes. Customers who are running Internet Explorer 7 are not affected by this vulnerability.

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

Yes. 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 section of this security update for more information about Internet Explorer Enhanced Security Configuration.

What is the Internet Explorer Enhanced Security Configuration?

Internet Explorer Enhanced Security Configuration is a group of preconfigured Internet Explorer settings that reduce the likelihood of a user or of an administrator downloading and running specially crafted Web content on a server. Internet Explorer Enhanced Security Configuration reduces this risk by modifying many security-related settings. This includes the settings on the Security tab and the Advanced tab in the Internet Options dialog box. Some of the important modifications include the following:

- * Security level for the Internet zone is set to High. This setting disables scripts, ActiveX controls, Microsoft Java Virtual Machine (MSJVM), and file downloads.
- * Automatic detection of intranet sites is disabled. This setting assigns all intranet Web sites and all Universal Naming Convention (UNC) paths that are not explicitly listed in the Local intranet zone to the Internet zone.
- * Install On Demand and non-Microsoft browser extensions are disabled. This setting prevents Web pages from automatically installing components and prevents non-Microsoft extensions from running.
- * Multimedia content is disabled. This setting prevents music, animations, and video clips from running.

For more information regarding Internet Explorer Enhanced Security Configuration, see the guide, *Managing Internet Explorer Enhanced Security Configuration*, at the following [Download Center](#).

What does the update do?

The update removes the vulnerability by making Microsoft Agent gracefully handle specially crafted URLs.

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

[NT] Microsoft Agent Remote Code Execution (MS07-020)

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 Security Bulletin MS07-020.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms07-020.msp>>

<http://www.microsoft.com/technet/security/bulletin/ms07-020.msp>

=====

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.