

[NT] Vulnerability in Microsoft Agent Allows Spoofing (MS05-032)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0066.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 06/15/05

To: list@securiteam.com

Date: 15 Jun 2005 16:11:31 +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 Agent Allows Spoofing (MS05-032)

SUMMARY

Microsoft Agent is "a software technology that enables an enriched form of user interaction that can make using and learning to use a computer easier and more natural. For more information, see the <http://www.microsoft.com/msagent/default.asp> Microsoft Agent Web site".

This vulnerability could enable an attacker to spoof trusted Internet content by using Microsoft's Agent.

DETAILS

Vulnerable Systems:

* Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4

<http://www.microsoft.com/downloads/details.aspx?FamilyId=6A7DEE96-F693-4C50-896D-2365873245A9>

Download the update

* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

<http://www.microsoft.com/downloads/details.aspx?FamilyId=F2247275-25F9-4937-97CD-9334135D6D79>

Securiteam: [NT] Vulnerability in Microsoft Agent Allows Spoofing (MS05-032)

Download the update

* Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=33E0A62D-395B-402C-A0A4-82E892E9B7AE>>

Download the update

* Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9BA306DC-9C31-432B-91E0-B057C9C1EEAE>>

Download the update

* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9BA306DC-9C31-432B-91E0-B057C9C1EEAE>>

Download the update

* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=5B38AF7A-3054-4EFD-9007-E4EB3B57179E>>

Download the update

* 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=BB35F2A8-B1D2-4B8E-BA94-DCD480DCD662>>

Download the update

* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=D092C628-ACCA-493C-9E20-1F50D1590725>>

Download the update

* 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.

This is a spoofing vulnerability that exists in the affected products and that could enable an attacker to spoof trusted Internet content. Users could believe that they are accessing trusted Internet content. However, they are accessing malicious Internet content such as a malicious Web site. An attacker would first have to persuade a user to visit the attacker's site to attempt to exploit this vulnerability.

Mitigating Factors for Microsoft Agent Vulnerability – CAN-2005-1214:

* 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 Web site. After they click the link, they would be prompted to perform several actions. An attack could only occur after they performed these actions.

* 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

Securiteam: [NT] Vulnerability in Microsoft Agent Allows Spoofing (MS05-032)

than users who operate with administrative user rights.

* By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode mitigates this vulnerability. See the FAQ section of this vulnerability for more information about Internet Explorer Enhanced Security Configuration.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could spoof trusted Internet content. Users could believe they are accessing trusted Internet content when in reality they are accessing malicious Internet content. Security prompts, as well as other types of Internet content, could be spoofed if an attacker is successfully able to exploit this vulnerability. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of the affected system.

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.

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

http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc_changes.asp
Enhanced Security Configuration. This mode mitigates this vulnerability.

What is 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 malicious 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 on the Advanced tab in the Internet Options dialog box. Some of the important modifications include the following:

* The 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

Securiteam: [NT] Vulnerability in Microsoft Agent Allows Spoofing (MS05–032)

and prevents non–Microsoft extensions from running.

* Multimedia content is disabled. This setting prevents music, animations, and video clips from running.

Workarounds for Microsoft Agent Vulnerability – CAN–2005–1214: Microsoft has tested the following workarounds. While 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.

* Set Internet and Local intranet security zone settings to High to disable running ActiveX controls in these zones.

You can help protect against this vulnerability by changing your settings for the Internet security zone to disable 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.
4. Repeat step 1 through step 3 and select the Local intranet security zone.

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 high security setting. See the Restrict Web sites to only your trusted Web sites workaround for information about how you can add sites to the Trusted sites zone.

Alternatively, you can change your settings to prompt before running ActiveX controls only. 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.

Securiteam: [NT] Vulnerability in Microsoft Agent Allows Spoofing (MS05–032)

4. Under Settings, in the Scripting section, under Active Scripting, click Prompt, 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 plugs-ins, click Prompt.

7. Click OK two times to return to Internet Explorer.

Impact of Workaround: There are side effects to disabling running ActiveX controls. Many Web sites that are on the Internet or on an intranet use ActiveX controls to provide additional functionality. Disabling running ActiveX controls is a global setting that affects all Internet and intranet sites. If you do not want to disable ActiveX controls for all sites, use the "Restrict Web sites to only your trusted Web sites" workaround.

* Restrict Web sites to only your trusted Web sites.

After you set Internet Explorer to disable ActiveX controls 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.

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 quotation marks). This is the site that will host the update, and it requires an ActiveX control to install the update.

Securiteam: [NT] Vulnerability in Microsoft Agent Allows Spoofing (MS05-032)

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1214>>
CAN-2005-1214

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-032.msp>>
<http://www.microsoft.com/technet/security/Bulletin/MS05-032.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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.