

[NT] Vulnerability in Microsoft Data Access Components Allows Code Execution (MS07-009)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00051.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2007 12:10:36 +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 Data Access Components Allows Code Execution
(MS07-009)

SUMMARY

A remote code execution vulnerability exists in the ADODB.Connection ActiveX control that is provided as part of the ActiveX Data Objects (ADO) and that is distributed in MDAC. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

DETAILS

Affected Software:

* Microsoft Data Access Components 2.5 Service Pack 3 on Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=EF163E3E-DD3B-4429-98A4-720DA2C96464>>
Download the update

* Microsoft Data Access Components 2.8 Service Pack 1 on Microsoft Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=6B0CDB65-AEF4-489F-B917-812D9F7687BD>>
Download the update

* Microsoft Data Access Components 2.8 on Microsoft Windows Server 2003 –

[NT] Vulnerability in Microsoft Data Access Components Allows Code Execution (MS07-009)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=34D24335-4EC0-49E7-9E3F-787F89DD7B1D>>

Download the update

* Microsoft Data Access Components 2.8 on Microsoft Windows Server 2003 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=58322D1B-A1A8-4BA6-BA1B-6649013CC324>>

Download the update

Non-Affected Software:

Microsoft Data Access Components 2.8 Service Pack 2 on Microsoft Windows XP Professional x64 Edition

Microsoft Data Access Components 2.8 Service Pack 2 on Microsoft Windows Server 2003 Service Pack 1

Microsoft Data Access Components 2.8 Service Pack 2 on Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

Microsoft Data Access Components 2.8 Service Pack 2 on Microsoft Windows Server 2003 x64 Edition

Windows Data Access Components 6.0 on Windows Vista

Tested Microsoft Windows Affected Components:

* Microsoft Data Access Components 2.7 Service Pack 1 when installed on Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=591B0967-C8AB-4B85-A9AF-C01E8D8E3ADC>>

Download the update

* Microsoft Data Access Components 2.8 when installed on Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=BC864245-175A-4B55-AB4A-FB5D0E03DCFC>>

Download the update

* Microsoft Data Access Components 2.8 Service Pack 1 when installed on Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=341859BF-8DAA-419B-88CD-E5E8EB4A5BAD>>

Download the update

Mitigating Factors for Microsoft Windows MDAC ActiveX Vulnerability – CVE-2006-5559:

* 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 the page. 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 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 logged on 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 section of this security update for more information about Internet Explorer Enhanced Security Configuration.

Workarounds for Microsoft Windows MDAC ActiveX Vulnerability – CVE-2006-5559:

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.

* Prevent the ADODB.Connection ActiveX Control from running in Internet Explorer

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 Registry Editor at your own risk.

1. Save the following text to a .reg file and then run it on the vulnerable client.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX  
Compatibility\{00000514-0000-0010-8000-00AA006D2EA4}]  
Compatibility Flags=dword:00000400
```

2. 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:

Group Policy collection
What is Group Policy Object Editor?
Core Group Policy tools and settings

Impact of Workaround: Disables some MDAC functionality from within Internet Explorer.

To Rollback:

Remove the above registry entry from the registry.

* Unregister the ADO ActiveX controls

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system.

[NT] Vulnerability in Microsoft Data Access Components Allows Code Execution (MS07-009)

Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

* At the command prompt run the following:

```
regsvr32 -u "%CommonProgramFiles%\System\ado\msado15.dll
```

Impact of Workaround: This will likely break lots of MDAC functionality, more intrusive than the killbit above.

To Rollback:

At the command prompt run the following:

```
regsvr32 "%CommonProgramFiles%\System\ado\msado15.dll
```

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

[NT] Vulnerability in Microsoft Data Access Components Allows Code Execution (MS07-009)

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.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security Bulletin MS07-009. The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms07-009.mspx>>
<http://www.microsoft.com/technet/security/bulletin/ms07-009.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:

[NT] Vulnerability in Microsoft Data Access Components Allows Code Execution (MS07-009)

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.