

[NT] Cumulative Security Update for Internet Explorer (MS05-052)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-10/0047.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 10/12/05

To: list@securiteam.com

Date: 12 Oct 2005 10:56:07 +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>

Cumulative Security Update for Internet Explorer (MS05-052)

SUMMARY

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

DETAILS

Affected Software:

- * 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 Windows Server 2003 with Service Pack 1 for Itanium-based Systems

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS05-052)

- * 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.

Tested Microsoft Windows Components:

Affected Components:

- * Internet Explorer 5.01 Service Pack 4 on Microsoft Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B1F0216C-0D62-4141-9DC7-3C7B06C3A30A>>

Download the update

- * Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 4 or on Microsoft Windows XP Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8F638D4A-670D-46C7-A7A1-1D1E3DC9732F>>

Download the update

- * Internet Explorer 6 for Microsoft Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=41CCCA21-5010-49FF-A2DD-CB365F6FD3C5>>

Download the update

- * Internet Explorer 6 for Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4739846F-C35D-4C62-8E1A-60E01F3B3A59>>

Download the update

- * Internet Explorer 6 for 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=44F43899-E897-4495-A4F1-73A4D48E001A>>

Download the update

- * Internet Explorer 6 for Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=24846F0A-0530-42D1-AC60-216C0260ACA3>>

Download the update

- * Internet Explorer 6 for Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=59575247-3E71-4595-92B9-4E45F6D324EF>>

Download the update

- * Internet Explorer 5.5 Service Pack 2 on Microsoft Windows Millennium Edition Review the FAQ section of this bulletin for details about this version.

- * Internet Explorer 6 Service Pack 1 on Microsoft Windows 98, on Microsoft Windows 98 SE, or on Microsoft Windows Millennium Edition Review the FAQ section of this bulletin for details about this version.

Caveats: <<http://support.microsoft.com/kb/896688>> Microsoft Knowledge Base Article 896688 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see <<http://support.microsoft.com/kb/896688>> Microsoft Knowledge Base Article 896688.

CVE Information:

COM Object Instantiation Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2127>>

CAN-2005-2127

Mitigating Factors for COM Object Instantiation Memory Corruption Vulnerability – CAN-2005-2127:

* 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.

* 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 ActiveX controls 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 98, and Outlook 2000 open 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 Enhanced Security Configuration. This mode mitigates this vulnerability. See the FAQ section for this security update for more information about Internet Explorer Enhanced Security Configuration.

Workarounds for COM Object Instantiation Memory Corruption Vulnerability – CAN-2005-2127:

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.

* 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 settings to prompt before running ActiveX controls or to disable ActiveX controls in the Internet and Local intranet security zone. To do this, follow these steps:

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS05–052)

1. 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. 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.

Note Disabling ActiveX controls 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 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 "Restrict Web sites to only your trusted Web sites" workaround.

* Set Internet and Local intranet security zone settings to High to prompt before running ActiveX controls 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.

Repeat steps 1 through 3 for the Local intranet security zone by clicking the Local intranet icon.

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

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS05–052)

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 "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 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.

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.

* Prevent COM objects from running in Internet Explorer

You can disable attempts to instantiate a COM object 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

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS05-052)

using Registry Editor incorrectly. Use Registry Editor at your own risk.

For detailed steps about preventing a control from running in Internet Explorer, see <<http://support.microsoft.com/kb/240797>> Microsoft Knowledge Base Article 240797. Follow these steps and create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer.

For example, to set the kill bit for a CLSID in the Msdds.dll, file that is included in this security update, 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\{EC444CB6-3E7E-4865-B1C3-0DE72EF39B3F}]  
"Compatibility Flags"=dword:00000400
```

You can apply this .reg file to individual systems by double-clicking it. You can also apply it across domains 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: There is no impact as long as the COM object is not intended to be used in Internet Explorer.

FAQ for COM Object Instantiation Memory Corruption Vulnerability –
CAN-2005-2127:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could remotely 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?

When Internet Explorer tries to instantiate certain COM objects as ActiveX controls, the COM objects may corrupt system memory in such a way that an

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS05-052)

attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system. In a Web-based attack scenario, an attacker would host a Web site that exploits 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 site. It could also be possible to display malicious Web content by using banner advertisements or by using other methods to deliver Web content to affected systems.

How could an attacker exploit the vulnerability?

An attacker could host a malicious Web site that is designed to exploit this vulnerability through Internet Explorer and then persuade a user to view the Web site.

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user is logged on and reading e-mail messages or that a user visits a Web site for any malicious action to occur. Therefore, any systems where e-mail messages are read or where Internet Explorer is used frequently, such as workstations or terminal servers, are at the most risk from this vulnerability.

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 this vulnerability. The security updates are available 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?

Because not all COM objects are designed to be accessed through Internet Explorer, this update sets the <<http://support.microsoft.com/kb/240797>> kill bit for a list of Class Identifiers (CLSIDs) in COM objects that have been found to exhibit similar behavior to the COM object Instantiation Memory Corruption Vulnerability that is addressed in <<http://go.microsoft.com/fwlink/?LinkId=45781>> Microsoft Security Bulletin MS05-038. To help protect customers, this update prevents these CLSIDs from being instantiated in Internet Explorer. For more information about kill bits, see <<http://support.microsoft.com/kb/240797>> Microsoft Knowledge Base Article 240797.

The Class Identifiers and corresponding COM objects are as follows.

BC5F1E51-5110-11D1-AFF5-006097C9A284 Blnmgrps.dll

F27CE930-4CA3-11D1-AFF2-006097C9A284 Blnmgrps.dll

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS05-052)

3BC4F3A7-652A-11D1-B4D4-00C04FC2DB8D Ciodm.dll
ECABAFC2-7F19-11D2-978E-0000F8757E2A Comsvcs.dll
283807B8-2C60-11D0-A31D-00AA00B92C03 Danim.dll
250770F3-6AF2-11CF-A915-008029E31FCD Htmlmarq.ocx
D24D4453-1F01-11D1-8E63-006097D2DF48 Mdt2dd.dll
03CB9467-FD9D-42A8-82F9-8615B4223E6E Mdt2qd.dll
598EBA02-B49A-11D2-A1C1-00609778EA66 Mpg4ds32.ax
8FE7E181-BB96-11D2-A1CB-00609778EA66 Msadds32.ax
4CFB5280-800B-4367-848F-5A13EBF27F1D Msbl1esen.dll
B3E0E785-BD78-4366-9560-B7DABE2723BE Msbl1fren.dll
208DD6A3-E12B-4755-9607-2E39EF84CFC5 Msbl1geen.dll
EC444CB6-3E7E-4865-B1C3-0DE72EF39B3F Msdds.dll
4FAAB301-CEF6-477C-9F58-F601039E9B78 Msdds.dll
6CBE0382-A879-4D2A-8EC3-1F2A43611BA8 Msdds.dll
F117831B-C052-11D1-B1C0-00C04FC2F3EF Msdtctm.dll
3050F667-98B5-11CF-BB82-00AA00BDCE0B Mshtml.dll
1AA06BA1-0E88-11D1-8391-00C04FBD7C09 Msoeacct.dll
F28D867A-DDB1-11D3-B8E8-00A0C981AEEB Msosvfbr.dll
6B7F1602-D44C-11D0-A7D9-AE3D17000000 Mswcrun.dll
7007ACCF-3202-11D1-AAD2-00805FC1270E Netshell.dll
992CFFA0-F557-101A-88EC-00DD010CCC48 Netshell.dll
00020420-0000-0000-C000-000000000046 Ole2disp.dll
0006F02A-0000-0000-C000-000000000046 Outllib.dll
ABBA001B-3075-11D6-88A4-00B0D0200F88 Psisdecn.dll
CE292861-FC88-11D0-9E69-00C04FD7C15B Qdvd.dll
6E227101-F799-11CF-9227-00AA00A1EB95 Repodbc.dll

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS05-052)

7057E952-BD1B-11D1-8919-00C04FC2C836 Shdocvw.dll

7007ACC7-3202-11D1-AAD2-00805FC1270E Shell32.dll

4622AD11-FF23-11D0-8D34-00A0C90F2719 Shell32.dll

98CB4060-D3E7-42A1-8D65-949D34EBFE14 Soa.dll

47C6C527-6204-4F91-849D-66E234DEE015 Srchui.dll

35CEC8A3-2BE6-11D2-8773-92E220524153 Stobject.dll

730F6CDC-2C86-11D2-8773-92E220524153 Stobject.dll

2C10A98F-D64F-43B4-BED6-DD0E1BF2074C Vdt70.dll

6F9F3481-84DD-4B14-B09C-6B4288ECCDE8 Vdt70.dll

8E26BFC1-AFD6-11CF-BFFC-00AA003CFDFC Vmhelper.dll

F0975AFE-5C7F-11D2-8B74-00104B2AFB41 Wbemads.dll

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

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CAN-2005-2127.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

Yes. When the security bulletin was released, Microsoft had received information that this vulnerability was being exploited.

Does applying this security update help protect customers from the code that has been published publicly that attempts to exploit this vulnerability?

Yes. This security update addresses the vulnerability that is currently being exploited. The vulnerability that has been addressed has been assigned the Common Vulnerability and Exposure number CAN-2005-2127.

How does this vulnerability relate to the vulnerability that is corrected by MS05-038?

Both are COM object Instantiation Memory Corruption vulnerabilities. However, this update also addresses new CLSIDs that were not addressed as part of MS05-038. MS05-038 helps protect against exploitation of the CLSIDs that are discussed in that bulletin.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-052.msp>>
<http://www.microsoft.com/technet/security/Bulletin/MS05-052.msp>

Securiteam: [NT] Cumulative Security Update for Internet Explorer (MS05-052)

=====

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.