

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00041.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 14 Dec 2005 18:27:35 +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 (MS05-054)

SUMMARY

This update resolves several newly-discovered, publicly and privately reported vulnerabilities. Each vulnerability is documented in its own section of this advisory.

If a user is logged on with administrative user rights, an attacker who successfully exploited the most severe of these vulnerabilities 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. 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.

A remote code execution vulnerability exists in the way Internet Explorer displays file download dialog boxes and accepts user input during interaction with a Web page. This interaction could be in the form of certain keystrokes that a user makes when visiting a Web page. A custom dialog box may also be positioned in front of a file download dialog box to make this more convincing. A user may also be persuaded to double-click an element of a Web page.

[NT] Cumulative Security Update for Internet Explorer (MS05–054)

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. However, significant user interaction is required to exploit this vulnerability.

An information disclosure vulnerability exists in the way Internet Explorer behaves in certain situations where an HTTPS proxy server requires clients to use Basic authentication. This vulnerability could allow an attacker to read Web addresses in clear text sent from Internet Explorer to a proxy server despite the connection being an HTTPS connection.

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.

A remote code execution vulnerability exists in the way Internet Explorer handles mismatched Document Object Model objects. 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

Vulnerable Systems:

- * 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
- * Microsoft Windows Server 2003 x64 Edition family
- * 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.

Note The security updates for Microsoft Windows Server 2003, Microsoft Windows Server 2003 Service Pack 1, and Microsoft Windows Server 2003 x64 Edition also apply to Microsoft Windows Server 2003 R2.

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

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4005B74A-D6E6-4A32-A3B1-276686B4A428>>

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=A8443CD2-D98D-427B-9F0E-BD7E19FCB994>>

Download the update

* Internet Explorer 6 for Microsoft Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E4B5BA57-D4F2-4798-9154-2869E371C9D1>>

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=9D70FB20-C7C9-43AF-A864-6DBC9A542CC6>>

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=1EE790B9-E596-4344-AEC3-FCB3289D7E9C>>

Download the update

* Internet Explorer 6 for Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8E9C23E5-7988-42DA-A8BD-2C1A534BF995>>

Download the update

* Internet Explorer 6 for Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E1652B4A-6339-4B31-8ACF-D2A844C24F70>>

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.

The software in this list has been tested to determine whether the versions are affected. Other versions either no longer include security update support or may not be affected. To determine the support life cycle for your product and version, visit the Microsoft Support Lifecycle Web site.

File Download Dialog Box Manipulation Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829>>

CAN-2005-2829:

A remote code execution vulnerability exists in the way Internet Explorer displays file download dialog boxes and accepts user input during interaction with a Web page. This interaction could be in the form of certain keystrokes that a user makes when visiting a Web page. A custom dialog box may also be positioned in front of a file download dialog box to make this more convincing. A user may also be persuaded to double-click an element of a Web page.

An attacker could exploit the vulnerability by constructing a malicious

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

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. However, significant user interaction is required to exploit this vulnerability.

Mitigating Factors for File Download Dialog Box Manipulation Vulnerability – <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829>
CAN-2005-2829:

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. For an attack to be successful, a user would then have to interact with the 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 Active Scripting and 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 File Download Dialog Box Manipulation Vulnerability – <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829>
CAN-2005-2829:

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.

[NT] Cumulative Security Update for Internet Explorer (MS05–054)

* Configure Internet Explorer to prompt before running Active Scripting or 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. If you are prompted to confirm that you want to change these settings, click Yes.
8. Click OK to return to Internet Explorer.

Note 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.

Impact of Workaround: There are side effects to prompting before running Active Scripting. Many Web sites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting 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 Active Scripting. 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 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 and Active Scripting. 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.

[NT] Cumulative Security Update for Internet Explorer (MS05–054)

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.

4. Click Custom Level.

5. Under Settings, in the Scripting section, under Active Scripting, click Prompt and then click OK.

6. If you are prompted to confirm that you want to change these settings, click Yes.

7. Click OK to return to Internet Explorer.

Impact of Workaround: There are side effects to prompting before running ActiveX Controls and Active Scripting. Many Web sites that are on the Internet or on an intranet use ActiveX or Active Scripting 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 or Active Scripting 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 or Active Scripting. 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, click Default Level, move the slider to Medium, and then click Sites.

Note Setting the level to Medium is a suggested added precaution. It may cause some Web sites to work incorrectly if you have placed sites in the Trusted sites zone that require the default setting of Low.

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.

FAQ for File Download Dialog Box Manipulation Vulnerability –
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829>>
CAN-2005-2829:

What is the scope of the vulnerability?

This is a remote code execution vulnerability that relies to a large extent on social engineering. 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. However, significant user interaction is required to exploit this vulnerability.

What causes the vulnerability?

This vulnerability relies to a large extent on social engineering and relies on the way that Internet Explorer displays file download dialog boxes and accepts user input during interaction with a Web page. This interaction could be in the form of certain keystrokes that a user makes when visiting a Web page. A custom dialog box may also be positioned in front of a file download dialog box to make this more convincing. A user may also be persuaded to double-click an element of a Web page.

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 and then persuade a user to view the Web site by using Internet Explorer. It should be noted that this vulnerability relies to a

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

large extent on social engineering and that a user would need to interact with the attacker's Web site.

What systems are primarily at risk from the vulnerability?

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

Are Windows 98, Windows 98 Second Edition, or Windows Millennium Edition critically affected by this vulnerability?

No. Although Windows 98, Windows 98 Second Edition, and Windows Millennium Edition do contain the affected component, the vulnerability is not critical because it requires significant user interaction. For more information about severity ratings, visit the following <http://go.microsoft.com/fwlink/?LinkId=21140> Web site.

What does the update do?

The update removes the vulnerability by making sure that the result of user interaction with a Web page or dialog box cannot be transferred to the file download dialog box.

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

No. Microsoft received information about this vulnerability through responsible disclosure.

HTTPS Proxy Vulnerability–

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829>
CAN-2005-2830:

An information disclosure vulnerability exists in the way Internet Explorer behaves in certain situations where an HTTPS proxy server requires clients to use Basic authentication. This vulnerability could allow an attacker to read Web addresses in clear text sent from Internet Explorer to a proxy server despite the connection being an HTTPS connection.

Mitigating Factors for HTTPS Proxy Vulnerability–

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829>
CAN-2005-2830:

- * This vulnerability only manifests itself if a client system is configured to use an authenticating proxy server that requires Basic authentication for HTTPS communications.
- * An attacker must be on the same network as the user.
- * An attacker would have no way of targeting this to a specific user. The information disclosure can happen only when a user uses an authenticating proxy server for HTTPS communications.

Workarounds for HTTPS Proxy Vulnerability–

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829>

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

CAN-2005-2830:

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.

* Do not use authenticating proxy servers that require Basic Authentication as a proxy for HTTPS communication

You can help protect against this vulnerability by not having proxy servers that require Basic authentication in your enterprise. Alternatively, you can make sure that you do not use authenticating proxy servers as a proxy for HTTPS communication.

Impact of Workaround: Applications that require Basic authentication might not work as unexpected.

FAQ for HTTPS Proxy Vulnerability–

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829>>

CAN-2005-2830:

What is the scope of the vulnerability?

This is an information disclosure vulnerability. This vulnerability could allow an attacker to read Web addresses in clear text sent from Internet Explorer to a proxy server despite the connection being an HTTPS connection. This proxy server also must require that client systems use Basic authentication to the proxy server.

What causes the vulnerability?

This vulnerability manifests itself if a client system is configured to use an authenticating proxy server that requires Basic authentication for HTTPS communications.

What might an attacker use the vulnerability to do?

This vulnerability could allow an attacker to read Web addresses in clear text sent from Internet Explorer to a proxy server despite the connection being an HTTPS connection. This proxy server also must require that client systems use Basic authentication to the proxy server.

What is HTTPS and Basic Authentication?

HTTPS is a protocol that helps secure HTTP communications. In Internet Explorer, when you visit a Web site and a yellow lock icon appears in the lower-right corner of the browser window, the current session is protected by HTTPS.

Basic authentication means that credentials are sent to the proxy server in clear text or encoded by using Base64 encoding. Base64 encoding is not an encryption technique and considered to be equal to clear text. For more information about different authentication methods, see the <http://go.microsoft.com/fwlink/?LinkId=56562>> product documentation.

What is a Proxy Server?

A proxy server is a server configured to act on behalf of assigned clients. When a client application makes a request for an object on the Internet, a proxy server on the private network responds by translating the request and passing it to the Internet. When a computer on the Internet responds, the proxy server passes that response back to the client application on the computer that made the request.

How could an attacker exploit the vulnerability?

An attacker could analyze network traffic between a client system and a proxy server that requires Basic authentication and that also handles HTTPS connections.

What systems are primarily at risk from the vulnerability?

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

Are Windows 98, Windows 98 Second Edition or Windows Millennium Edition critically affected by this vulnerability?

No. Although Windows 98, Windows 98 Second Edition, and Windows Millennium Edition do contain the affected component, the vulnerability is not critical. For more information about severity ratings, visit the following <http://go.microsoft.com/fwlink/?LinkId=21140> Web site.

What does the update do?

The update removes the vulnerability by making sure that Internet Explorer uses the HTTPS connection to the proxy server when sending URLs.

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

Yes. This vulnerability has been publicly disclosed.

COM Object Instantiation Memory Corruption Vulnerability –

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2831>
CAN-2005-2831:

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.

Mitigating Factors for COM Object Instantiation Memory Corruption Vulnerability –

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2831>
CAN-2005-2831:

* 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 – <<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2831>> CAN-2005-2831:

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:

1. In Internet Explorer, click Internet Options on the Tools menu.
2. Click the Security tab.
3. Click Internet, and then click Custom Level.

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

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. If you are prompted to confirm that you want to change these settings, click Yes.
8. Click OK 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.

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.

4. Click Custom Level.
5. Under Settings, in the Scripting section, under Active Scripting, click Prompt and then click OK.
6. If you are prompted to confirm that you want to change these settings, click Yes.
7. Click OK 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 "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, click Default Level, move the slider to Medium, and then click Sites.

Note Setting the level to Medium is a suggested added precaution. It may cause some Web sites to work incorrectly if you have placed sites in the Trusted sites zone that require the default setting of Low.

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.

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

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 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 Avifil32.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.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX  
Compatibility\{0002000D-0000-0000-C000-000000000046}]  
"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.

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

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 –
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2831>>
CAN-2005-2831:

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 the system state in such a way that an 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 is logged on and 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?

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

Because not all COM objects are designed to be accessed through Internet Explorer, this update sets the [kill bit](http://support.microsoft.com/kb/240797) 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 [Microsoft Security Bulletin MS05-052](http://go.microsoft.com/fwlink/?LinkId=50690). To help protect customers, this update prevents these CLSIDs from being instantiated in Internet Explorer. For more information about kill bits, see [Microsoft Knowledge Base Article 240797](http://support.microsoft.com/kb/240797).

The Class Identifiers and corresponding COM objects are as follows.

Class Identifier

COM object

0002000D-0000-0000-C000-000000000046 – Avifil32.dll
ECABAF0-7F19-11D2-978E-0000F8757E2A – Comsvcs.dll
ECABB0AB-7F19-11D2-978E-0000F8757E2A – Comsvcs.dll
3050F4F5-98B5-11CF-BB82-00AA00BDCE0B – Mshtml.dll
00020421-0000-0000-C000-000000000046 – Ole2disp.dll
00020422-0000-0000-C000-000000000046 – Ole2disp.dll
00020423-0000-0000-C000-000000000046 – Ole2disp.dll
00020424-0000-0000-C000-000000000046 – Ole2disp.dll
00020425-0000-0000-C000-000000000046 – Ole2disp.dll
DF0B3D60-548F-101B-8E65-08002B2BD119 – Ole2disp.dll / Oleaut32.dll
0006F071-0000-0000-C000-000000000046 – Outllib.dll
2D2E24CB-0CD5-458F-86EA-3E6FA22C8E64 – Quartz.dll
51B4ABF3-748F-4E3B-A276-C828330E926A – Quartz.dll
E4979309-7A32-495E-8A92-7B014AAD4961 – Quartz.dll
62EC9F22-5E30-11D2-97A1-00C04FB6DD9A – Repodbc.dll
6E2270FB-F799-11CF-9227-00AA00A1EB95 – Repodbc.dll
6E227109-F799-11CF-9227-00AA00A1EB95 – Repodbc.dll
6E22710A-F799-11CF-9227-00AA00A1EB95 – Repodbc.dll
6E22710B-F799-11CF-9227-00AA00A1EB95 – Repodbc.dll
6E22710C-F799-11CF-9227-00AA00A1EB95 – Repodbc.dll
6E22710D-F799-11CF-9227-00AA00A1EB95 – Repodbc.dll
6E22710E-F799-11CF-9227-00AA00A1EB95 – Repodbc.dll
6E22710F-F799-11CF-9227-00AA00A1EB95 – Repodbc.dll
B1D4ED44-EE64-11D0-97E6-00C04FC30B4A – Repodbc.dll
D675E22B-CAE9-11D2-AF7B-00C04F99179F – Repodbc.dll
00021401-0000-0000-C000-000000000046 – Shell.dll

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

No. Microsoft received information about this vulnerability through responsible disclosure.

How does this vulnerability relate to one of the vulnerabilities that are corrected by MS05-038 and MS05-052?

Both security bulletins address COM object Instantiation Memory Corruption vulnerabilities. However, this update also addresses new CLSIDs that were

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

not addressed as part of MS05-038 and MS05-052. MS05-038 and MS05-052 help protect against exploitation of the CLSIDs that are discussed in those bulletins.

Mismatched Document Object Model Objects Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1790>>

CAN-2005-1790:

A remote code execution vulnerability exists in the way Internet Explorer handles mismatched Document Object Model objects. 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.

Mitigating Factors for Mismatched Document Object Model Objects Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1790>>

CAN-2005-1790:

* 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 of this bulletin

[NT] Cumulative Security Update for Internet Explorer (MS05–054)

for more information about Internet Explorer Enhanced Security Configuration.

Workarounds for Mismatched Document Object Model Objects Memory Corruption Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1790>>
CAN-2005-1790:

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 Active Scripting or 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. If you are prompted to confirm that you want to change these settings, click Yes.
8. Click OK to return to Internet Explorer.

Note 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.

Impact of Workaround: There are side effects to prompting before running Active Scripting. Many Web sites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting 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 Active Scripting. 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 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 and Active Scripting. 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.

4. Click Custom Level.
5. Under Settings, in the Scripting section, under Active Scripting, click Prompt and then click OK.
6. If you are prompted to confirm that you want to change these settings, click Yes.
7. Click OK to return to Internet Explorer.

Impact of Workaround: There are side effects to prompting before running ActiveX Controls and Active Scripting. Many Web sites that are on the Internet or on an intranet use ActiveX or Active Scripting 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 or Active Scripting 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 or Active Scripting. 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

[NT] Cumulative Security Update for Internet Explorer (MS05–054)

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, click Default Level, move the slider to Medium, and then click Sites.

Note Setting the level to Medium is a suggested added precaution. It may cause some Web sites to work incorrectly if you have placed sites in the Trusted sites zone that require the default setting of Low.

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.

FAQ for Mismatched Document Object Model Objects Memory Corruption Vulnerability – CAN–2005–1790:

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 handles mismatched Document Object Model objects it may corrupt system memory in such a way that an attacker could execute arbitrary code.

For example, when Internet Explorer displays a Web page that contains an onLoad event that points to a Window object, system memory may be corrupted in such a way that an 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

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

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 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.

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?

The update removes the vulnerability by modifying the way that Internet Explorer handles Mismatched Document Object Model Objects.

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-2005-1790.

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-2005-1790.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

[NT] Cumulative Security Update for Internet Explorer (MS05-054)

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-054.msp>>

<http://www.microsoft.com/technet/security/Bulletin/MS05-054.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@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.

-
- Prev by Date: [*\[EXPL\] SimpleBBS Command Execution \(Exploit\)*](#)
 - Next by Date: