

[NT] Vulnerability in Windows Shell Allows Remote Code Execution (MS05-008)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0031.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/09/05

To: list@securiteam.com

Date: 9 Feb 2005 18:23:02 +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 Windows Shell Allows Remote Code Execution (MS05-008)

SUMMARY

A privilege elevation vulnerability exists in Windows because of the way that Windows handles drag-and-drop events. An attacker could exploit the vulnerability by constructing a malicious Web page. This malicious Web page could potentially allow an attacker to save a file on the user's system if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, user interaction is required to exploit this vulnerability.

DETAILS

Affected Software:

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3B6A6CC1-CCE4-4462-A0D2-E88D38DEF807>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=865B5D9D-FC5B-4F91-A860-2C35A025A907>>

Securiteam: [NT] Vulnerability in Windows Shell Allows Remote Code Execution (MS05-008)

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B6DAA99A-6E0B-477D-99E9-5237BCF57762>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9EE7FF53-20EC-4B75-A255-72DD0AB52FF3>>

Download the update

* Microsoft Windows Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=80AA33F4-E5B0-42A6-844B-F80D6168E25E>>

Download the update

* Microsoft Windows Server 2003 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9EE7FF53-20EC-4B75-A255-72DD0AB52FF3>>

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.

CVE Information:

Drag-and-Drop Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0053>>

CAN-2005-0053

Mitigating Factors:

* 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 could also attempt to compromise a Web site to have it display a Web page with malicious content. An attacker would have no way to force users to visit a 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 or to a site that has been compromised by the attacker.

* This vulnerability allows an attacker to put malicious code on the user's system in specified locations. An attack could only occur after the user ran this code by restarting the system, by logging off and then logging back on to the system, or by unintentionally running the code that the attacker saved locally on the system.

* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

* By default, Microsoft Outlook Express 6, Outlook 2000, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone.

Outlook Express 5.5 Service Pack 2 opens HTML e-mail messages in the Restricted sites zone if Microsoft Security Bulletin

<<http://www.microsoft.com/technet/security/bulletin/MS04-018.msp>>

MS04-018 has been installed. The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability.

The risk of attack from the HTML e-mail vector can be significantly reduced if you meet all the following conditions:

* Install the update that is included with Microsoft Security Bulletin

<<http://www.microsoft.com/technet/security/bulletin/MS03-040.msp>>

MS03-040 or a later Cumulative Security Update for Internet Explorer.

* Use the Microsoft Outlook E-mail Security Update, use Microsoft Outlook Express 6 or a later version, or use Microsoft Outlook 2000 Service Pack 2 or a later version in its default configuration.

* 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 vulnerability for more information about Internet Explorer Enhanced Security Configuration.

Workarounds:

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.

* Disable Drag and Drop or copy and paste files in Internet Explorer
Disable Drag and Drop or copy and paste files in Internet Explorer by following these steps:

1. Obtain and install the <<http://go.microsoft.com/fwlink/?LinkId=31851>> MS04-038 Cumulative Security Update for Internet Explorer. This security update must be installed for these configuration steps to be effective.

2. Disable the Drag and drop or copy and paste files option in the Internet and Intranet Web content zones. Disable the Drag and drop or copy and paste files option in the Internet and local intranet zone. To do this, follow these steps:

1. In Internet Explorer, click Internet Options on the Tools menu, and then click the Security tab.
2. In the Select a Web content zone to specify its security settings box, click Internet, and then click Custom Level.
3. In the Settings box, locate the Drag and drop or copy and paste files option under Miscellaneous. Make a note of your current setting.
4. Under Drag and drop or copy and paste files, click Disable, and then click OK.
5. Click Yes, and then click OK two times.

Note Repeat these steps for the local intranet zone by clicking Local intranet instead of Internet in step 2. These steps are also outlined in <<http://support.microsoft.com/kb/888534>> Microsoft Knowledge Base Article 888534 where steps on how to restore your previous drag and drop or copy and paste files setting are outlined.

* 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 high security setting.

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.
4. Under Settings, in the ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt.
5. In the Scripting section, under Active Scripting, click Prompt, and then click OK.
6. Click Local intranet, and then click Custom Level.
7. Under Settings, in the ActiveX controls and plug-ins section, under Run ActiveX controls and plug-ins, click Prompt.
8. In the Scripting section, under Active Scripting, click Prompt.
9. 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 "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.

* Read e-mail messages in plain text format if you are using Outlook 2002 or a later version, or Outlook Express 6 SP1 or a later version, to help protect yourself from the HTML e-mail attack vector.

Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or a later version and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 or a later version can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only.

Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For more information about how to enable this setting in Outlook 2002, see <<http://support.microsoft.com/kb/307594>> Microsoft Knowledge Base Article 307594.

For information about this setting in Outlook Express 6, see <<http://support.microsoft.com/kb/291387>> Microsoft Knowledge Base Article 291387.

Impact of Workaround: E-mail messages that are viewed in plain text format will not contain pictures, specialized fonts, animations, or other rich content. Additionally:

- * The changes are applied to the preview pane and to open messages.
- * Pictures become attachments so that they are not lost.
- * Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.

Frequently Asked Questions:

What is the scope of the vulnerability?

This vulnerability involves drag and drop events in Windows. An attacker who successfully exploited this vulnerability could cause an executable file to be saved on the user's system. The user would not receive a dialog box requesting approval for the download. To exploit this vulnerability, an attacker would have to host a malicious Web site that contained a Web page that was designed to exploit this vulnerability and then persuade a user to visit that site. If the user took certain actions on that Web

page, executable files of the attacker's choice could be saved in specified locations on the user's system.

What causes the vulnerability?

Drag-and-Drop technology incorrectly validates some dynamic HTML (DHTML) events. This vulnerability permits a file to be downloaded to the user's system after the user clicks a link.

What are DHTML events?

DHTML events are special actions that are provided by the DHTML Object Model. These events can be used in script code to add dynamic content to a Web site. For more information about DHTML events, see the product documentation.

How could an attacker exploit the vulnerability?

An attacker who successfully exploited this vulnerability could save code of their choice to the user's local file system. Although this code could not be run through this vulnerability directly, the operating system might open the file if it is saved to a sensitive location, or a user may open the file inadvertently and cause the attacker's code to run.

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user is logged on and reading e-mail or visiting Web sites for any malicious action to occur. Therefore, any systems where e-mail is read or where Internet Explorer is used frequently, such as users workstations or terminal servers, are at the most risk from this vulnerability. Systems that are not typically used to read e-mail or to visit Web sites, such as most server systems, are at a reduced risk.

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

Yes. By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode 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 the Advanced tab in the Internet Options dialog box. Some of the important modifications include the following:

- * Security level for the Internet zone is set to High. This setting disables scripts, ActiveX controls, Microsoft Java Virtual Machine (MSJVM), HTML content, 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.

Securiteam: [NT] Vulnerability in Windows Shell Allows Remote Code Execution (MS05-008)

* Install On Demand and non-Microsoft browser extensions are disabled. This setting prevents Web pages from automatically installing components and prevents non-Microsoft extensions from running.

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

What does the update do?

The update removes the vulnerability by modifying the way that Windows validates some drag and drop events.

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

Yes. This vulnerability has been publicly disclosed. This vulnerability has been assigned Common Vulnerability and Exposure number CAN-2005-0053.

Note The update for the Drag-and-Drop Vulnerability – CAN-2005-0053 also addresses the following publicly disclosed issues: CAN-2004-0985, CAN-2004-0839, and CAN-2003-1027.

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 tries 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-2005-0053.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS05-008.msp>>
<http://www.microsoft.com/technet/security/bulletin/MS05-008.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.