

[NT] Windows Media Player Remote Code Execution (MS06-005)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00051.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2006 11:59:46 +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>

Windows Media Player Remote Code Execution (MS06-005)

SUMMARY

Windows Media Player has a remote code execution due to bad processing of bitmap files.

A specially crafted bitmap file (.bmp) could potentially allow remote code execution if found on a Web site or in an e-mail message. This allows the attacker to completely take over the attacked system but only with significant user interaction.

DETAILS

Vulnerable Systems:

* Windows Media Player for XP on Microsoft Windows XP Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=110054F2-244D-4036-B98C-E951CBA7E9BA>>

Download the update

* Windows Media Player 9 on Microsoft Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8F9EEF16-04F7-4DA8-A0EF-1797B52D0B4B>>

Download the update

* Windows Media Player 9 on Microsoft Windows Server 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8F9EEF16-04F7-4DA8-A0EF-1797B52D0B4B>>

[NT] Windows Media Player Remote Code Execution (MS06-005)

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.

* Microsoft Windows Media Player 7.1 when installed on Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=26A0B9E1-1242-4E55-B3D4-8377B83257C6>>

Download the update

* Microsoft Windows Media Player 9 when installed on Windows 2000 Service Pack 4 or Windows XP Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=8F9EEF16-04F7-4DA8-A0EF-1797B52D0B4B>>

Download the update

* Microsoft Windows Media Player 10 when installed on Windows XP Service Pack 1 or Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=182735E1-9382-4F2E-A624-D2316A96B411>>

Download the update

Immune Systems:

* Windows Media Player 6.4 on all Microsoft Windows operating systems

* Windows Media Player 10 on Microsoft Windows Server 2003 Service Pack 1

* Microsoft Windows XP Professional x64 Edition

* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

* Microsoft Windows Server 2003 x64 Edition

Mitigating Factors for Windows Media Player Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0006>>

CVE-2006-0006:

* Windows Media Player is not the default handler for .bmp files.

* When using Microsoft Windows 2000 Service Pack 4 with Windows Media Player 7.1 or Windows XP Service Pack 1 with Windows Media Player 8, users are not vulnerable in a Web-based attack. Users are still vulnerable if a user downloads and installs a malicious Windows Media Player Skin.

* In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to attempt 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 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.

* In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted file to the user and by persuading the user to open the file. Windows Media Player is not the default handler for .bmp files. In order for the exploit to take place, the user would have to save the .bmp file to the desktop and open it using Windows Media Player.

* 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 affected than users who operate with administrative user rights.

Workarounds for Windows Media Player Vulnerability –

<<http://www.microsoft.com/technet/security/Bulletin/MS06-005.mspx>>
CVE-2006-0006:

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.

Note The following steps require Administrator privileges. We recommend that you restart the computer after you apply this workaround. Alternatively, you can log out and log back in after you apply the workaround. However, we do recommend that you restart the computer.

Back up and remove the WMZ registry key

Removing the WMZ registry key helps protect the affected system from attempts to exploit this vulnerability. To backup and remove the WMZ registry key, follow these steps:

Note Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Note We recommend backing up the registry before you edit it.

1. Click Start, click Run, type regedit" (without the quotation marks), and then click OK.
2. Expand HKEY_CLASSES_ROOT, and then click .WMZ.
3. Click File, and then click Export.
4. In the Export Registry File dialog box, type a file name in the File Name box, and then click Save.
5. Click Edit, then click Delete to remove the registry key.
6. In the Confirm Key Delete dialog box, you receive a Are you sure you want to delete this key and all of its subkeys message. Click Yes.

Note Removing the skin file association needs to be done in addition to at least one of the workarounds listed below.

Impact of Workaround: This workaround disables the Media Player skin file association but does not prevent users from applying alternate skins that are already present in their default skins directory (%Programfiles%\Windows Media Player\skins).

Modify the Access Control List on the DirectX Filter Graph no thread registry key

Modifying the Access Control List on the Filter Graph no thread registry key helps protect the affected system from attempts to exploit this vulnerability. To modify the Filter Graph no Thread Splitter registry key, follow these steps.

Note Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Note We recommend backing up the registry before you edit it.

For Windows 2000

Note Make a note of the permissions that are listed in the dialog box so that you can restore them to their original values at a later time

1. Click Start, click Run, type "regedt32" (without the quotation marks), and then click OK.
2. Expand HKEY_CLASSES_ROOT, expand CLSID, and then click { E436EBB8-524F-11CE-9F53-0020AF0BA770}.
3. Click Security, and then click Permissions.
4. Click to clear the Allow Inheritable Permissions from the parent to propagate to this object check box. You are prompted to click Copy, Remove, or Cancel. Click Remove, and then click OK.
5. You receive a message that states that no one will be able to access this registry key. Click Yes when you are prompted to do so.

For Windows XP Service Pack 1 or later operating systems

Note Make a note of the permissions that are listed in the dialog box so that you can restore them to their original values at a later time

1. Click Start, click Run, type "regedit" (without the quotation marks), and then click OK.
2. Expand HKEY_CLASSES_ROOT, expand CLSID, and then click { E436EBB8-524F-11CE-9F53-0020AF0BA770}.
3. Click Edit, and then click Permissions.
4. Click Advanced.
5. Click to clear the Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here. check box. You are prompted to click Copy, Remove, or Cancel. Click Remove, and then check OK.
6. You receive a message that states that no one will be able to access this registry key. Click Yes, and then click OK to close the Permissions for { E436EBB8-524F-11CE-9F53-0020AF0BA770} dialog box.

Note If you have backed up and removed the DirectX Filter Graph no thread registry key, you do not need to modify the Access Control List on the DirectX Filter Graph no thread registry key.

Impact of Workaround: This workaround disables image rendering and audio and video playback in any number of DirectX-enabled applications.

Backup and remove the DirectX Filter Graph no thread registry key
Removing the Filter Graph no thread registry key helps protect the affected system from attempts to exploit this vulnerability. To backup and remove the Filter Graph no thread registry key, follow these steps:

Note Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.

Note We recommend backing up the registry before you edit it.

1. Click Start, click Run, type regedit" (without the quotation marks), and then click OK.
2. Expand HKEY_CLASSES_ROOT, expand CLSID, and then click {E436EBB8-524F-11CE-9F53-0020AF0BA770}.
3. Click File, and then click Export.
4. In the Export Registry File dialog box, type a file name in the File Name box, and then click Save.
5. Click Edit, and then click Delete to remove the registry key.
6. In the Confirm Key Delete dialog box, you receive a Are you sure you want to delete this key and all of its subkeys message. Click Yes.

Note If you have backed up and remove the DirectX Filter Graph no thread registry key, you do not need to modify the Access Control List on the DirectX Filter Graph no thread registry key

Impact of Workaround: This workaround disables image rendering and audio and video playback in any number of DirectX-enabled applications.

Un-register Quartz.dll

Un-registering the Quartz.dll registry key helps protect the affected system from attempts to exploit this vulnerability. To modify the Quartz.dll registry key, follow these steps.

Note This workaround is intended to help protect against Web-based exploit vectors and is not effective against exploits that have Windows Metafile images embedded in Microsoft Word documents and other similar attack vectors.

[NT] Windows Media Player Remote Code Execution (MS06–005)

1. Click Start, click Run, type "regsvr32 -u %windir%\system32\quartz.dll" (without the quotation marks), and then click OK.
2. When a dialog box appears that confirms that the process has been successful, click OK.

Impact of Workaround: This workaround disables image rendering and audio and video playback in any number of DirectX-enabled applications.

FAQ for Windows Media Player Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0006>>
CVE-2006-0006:

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.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability 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 affected than users who operate with administrative user rights.

What causes the vulnerability?

An unchecked buffer in the bitmap (.bmp) image parsing function within Windows Media Player.

What is Windows Media Player?

Windows Media Player is a feature of the Windows operating system for personal computers. It is used for playing audio and video.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system.

How could an attacker exploit the vulnerability?

In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to attempt 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 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.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted file to the user and by persuading the user to open the file. Windows Media Player is not the default handler for .bmp files. In order for the exploit to take place, the user would have to save

[NT] Windows Media Player Remote Code Execution (MS06-005)

the .bmp file to the desktop and open it using Windows Media Player.

An attacker could also attempt to exploit this vulnerability by embedding a specially crafted Windows Media Player (.wmp) image within another file, such as a Word document and convince a user to open this document.

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers could be at more risk if users who do not have sufficient administrative permissions are given the ability to log on to servers and to run programs. However, best practices strongly discourage allowing this.

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

Yes. This vulnerability is critical for Windows Media Player 9 on Windows 98, Windows 98 Second Edition, and Windows Millennium Edition. Critical security updates for these platforms may not be available concurrently with the other security updates provided as part of this security bulletin. They will be made available as soon as possible following the release. When these security updates are available, you will be able to download them only 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 the .bmp image parser validates the length of a field before it passes it to the allocated buffer.

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

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

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

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

The original article can be found at:

<http://www.microsoft.com/technet/security/Bulletin/MS06-005.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-005.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.