

[NT] Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06-078)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00016.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 13 Dec 2006 18:27:15 +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 Media Format Could Allow Remote Code Execution
(MS06-078)

SUMMARY

A remote code execution vulnerability exists in Windows Media Format Runtime due to the way it handles one of the following file formats: Advanced Systems Format (ASF) and Advanced Stream Redirector (ASX). An attacker could exploit the vulnerability by constructing specially crafted Windows Media Player content that could potentially allow remote code execution if a user visits a malicious Web site or opens an e-mail message with malicious content. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

DETAILS

Affected Software:

Microsoft Windows Media Format 7.1 through 9.5 Series Runtime on the following operating system versions:

- * Microsoft Windows 2000 Service Pack 4 – Download the update (KB923689)
- * Microsoft Windows XP Service Pack 2 – Download the update (KB923689)
- * Microsoft Windows XP Professional x64 Edition – Download the update (KB923689)

[NT] Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06-078)

- * Microsoft Windows Server 2003 or Microsoft Windows Server 2003 Service Pack 1 – Download the update (KB923689)
- * Microsoft Windows Server 2003 x64 Edition – Download the update (KB923689)

Microsoft Windows Media Format 9.5 Series Runtime x64 Edition on the following operating system versions:

- * Microsoft Windows XP Professional x64 Edition – Download the update (KB923689)
- * Microsoft Windows Server 2003 x64 Edition – Download the update (KB923689)

Microsoft Windows Media Player 6.4:

- * Windows 2000 Service Pack 4 – Download the update (KB925398)
- * Microsoft Windows XP Service Pack 2 – Download the update (KB925398)
- * Microsoft Windows XP Professional x64 Edition Download the update (KB925398)
- * Microsoft Windows Server 2003 or on Microsoft Windows Server 2003 Service Pack 1 Download the update (KB925398)
- * Microsoft Windows Server 2003 x64 Edition Download the update (KB925398)

Non-Affected Software:

- * Windows Vista
- * Microsoft Windows 2003 For Itanium-Based Systems and Windows Server 2003 with SP1 for Itanium-based Systems
- * Windows Media Format 11 Series when installed on all Microsoft Operating Systems

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

Windows Media Format ASF Parsing Vulnerability – CVE-2006-4702:

A remote code execution vulnerability exists in Windows Media Format Runtime due to the way it handles Advanced Systems Format (ASF) files. An attacker could exploit the vulnerability by constructing specially crafted Windows Media Player content that could potentially allow remote code execution if a user visits a malicious Web site or opens an e-mail message with malicious content. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for Windows Media Format ASF Parsing Vulnerability – CVE-2006-4702:

* In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site,

[NT] Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06-078)

typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site.

* An attacker who successfully exploited this vulnerability could gain the same user rights as the 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.

* Windows Media Format 11 Runtime is not affected by this vulnerability and could be used to prevent an attempt to exploit this vulnerability.

Workarounds for Windows Media Format ASF Parsing Vulnerability – CVE-2006-4702:

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.

* Prevent the Microsoft Windows Media Player ActiveX controls from running in Internet Explorer.

You can help prevent attempts to instantiate this ActiveX control 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 that you can use to prevent a control from running in Internet Explorer, see <<http://support.microsoft.com/kb/240797>> Microsoft Knowledge Base Article 240797. Follow these steps in this article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer.

Windows Media Player 6.4

To set the kill bit for a CLSID with a value of {22D6F312-B0F6-11D0-94AB-0080C74C7E95}, 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\{22D6F312-B0F6-11D0-94AB-0080C74C7E95}]
```

[NT] Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06-078)

"Compatibility Flags"=dword:00000400

Windows Media Player 7.1, 9 and 10

To set the kill bit for a CLSID with a value of {6BF52A52-394A-11D3-B153-00C04F79FAA6}, 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\{6BF52A52-394A-11D3-B153-00C04F79FAA6}]
```

"Compatibility Flags"=dword:00000400

You can apply this .reg file to individual systems by double-clicking it. You can also apply it across domains by using Group Policy. For more information about Group Policy, visit the following Microsoft Web sites:

<<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: Web sites that use the Windows Media Player ActiveX Controls may no longer display or function correctly.

FAQ for Windows Media Format ASF Parsing Vulnerability – CVE-2006-4702:

What is the scope of the vulnerability?

A remote code execution vulnerability exists in the Windows Media Format Runtime due to the way it handles the processing of Advanced Systems Format files (ASF). An attacker could exploit the vulnerability by constructing specially crafted Windows Media Format content that could potentially allow remote code execution if a user visits a malicious Web site or opens a specially crafted ASF format file in an e-mail message.

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

[NT] Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06-078)

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 overrun in the ASF processing code within Windows Media Format Runtime.

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 is Windows Media Format Runtime?

The Microsoft Windows Media Format Runtime provides information and tools for applications which use Windows Media content. For more information, see the <<http://msdn.microsoft.com/windowsmedia/TechPages/default.aspx>> product documentation.

What is Advanced Systems Format (ASF)?

ASF (Advanced Systems Format) is a file format that stores audio and video information and is specially designed to run over networks like the Internet. It is compressed format that contains streaming audio, video, slide shows, and synchronized events. ASF enables content to be delivered to you as a continuous flow of data. ASF files may have the file extension ASF, WMV, or WMA.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities 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.

How could an attacker exploit the vulnerability?

An attacker could host a specially crafted Web site that is designed to exploit these vulnerabilities through Internet Explorer and then persuade a user to view the Web site. This can also include Web sites that accept user-provided content or advertisements, Web sites that host user-provided content or advertisements, and compromised Web sites. These Web sites could contain specially crafted content that could exploit these vulnerabilities. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or in an Instant Messenger message that takes users to the attacker's Web site. It could also be possible to display specially crafted 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.

What systems are primarily at risk from the vulnerability?

[NT] Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06-078)

Workstations and terminal servers are primarily at risk. Servers could be at more risk if administrators allow users to log on to servers and to run programs. However, best practices strongly discourage allowing this.

What does the update do?

The update removes the vulnerability by modifying the way that Windows Media Format Runtime validates the length of data in the media data before passing the file 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.

Windows Media Format ASX Parsing Vulnerability – CVE-2006-6134:
A remote code execution vulnerability exists in Windows Media Format Runtime due to the way it handles certain elements contained in Advanced Stream Redirector (ASX) files. An attacker could exploit the vulnerability by constructing a specially crafted ASX file that could allow remote code execution if a user visits a malicious Web site, where specially crafted ASX files are used to launch Windows Media player, or if a user clicks on a URL pointing to a specially crafted ASX file. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for Windows Media Format ASX Parsing Vulnerability – CVE-2006-6134:

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.

* In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site.

[NT] Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06-078)

* By default, all supported versions of Microsoft Outlook and Microsoft Outlook Express open HTML e-mail messages in the Restricted sites zone. The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing Active Scripting and ActiveX controls from being used when reading HTML e-mail. However, if a user clicks on a link within an e-mail they could still be vulnerable to this issue through the Web-based attack scenario. Similarly, a user would still be at risk if opening an e-mail attachment.

* Windows Media Format 11 Runtime, Windows Media Format Runtime 7.1, and Windows Media Player 6.4 are not affected by this vulnerability.

Workarounds for Windows Media Format ASX Parsing Vulnerability – CVE-2006-6134:

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.

* Install Windows Media Player 11, which includes Windows Media Format Runtime 11

Install Windows Media Player 11 on Microsoft Windows XP Home Edition Service Pack 2, Windows XP Professional Service Pack 2, Windows XP Tablet PC Edition 2005, Windows XP Media Center Edition 2005 with KB900325, or Windows XP Professional x64 Edition. For more information about Windows Media Player 11 you can visit the <http://www.microsoft.com/windows/windowsmedia/player/11/default.aspx> Windows Media Player Home Web page.

Impact of Workaround: None.

* Prevent the Microsoft Windows Media Player ActiveX controls from running in Internet Explorer.

You can help prevent attempts to instantiate this ActiveX control in Internet Explorer by setting the kill bit for the control in the registry. This workaround will not provide protection from all attack vectors.

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 that you can use to prevent a control from running in Internet Explorer, see <http://support.microsoft.com/kb/240797> Microsoft

[NT] Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06-078)

Knowledge Base Article 240797. Follow these steps in this article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer.

Windows Media Player 9 and 10

To set the kill bit for a CLSID with a value of {6BF52A52-394A-11D3-B153-00C04F79FAA6}, 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\{6BF52A52-394A-11D3-B153-00C04F79FAA6}]
```

```
"Compatibility Flags"=dword:00000400
```

You can apply this .reg file to individual systems by double-clicking it. You can also apply it across domains by using Group Policy. For more information about Group Policy, visit the following Microsoft Web sites:

Note: You must restart Internet Explorer for your changes to take effect.

Impact of Workaround: When you disable the Windows Media Player ActiveX control, pages using this control will no longer function as designed. This prevents any content from being played through the control, including audio and video

FAQ for Windows Media Format ASX Parsing Vulnerability – CVE-2006-6134:

What is the scope of the vulnerability?

A remote code execution vulnerability exists in Windows Media Format Runtime due to the way it handles certain elements contained in Advanced Stream Redirector (ASX) files. An attacker could exploit the vulnerability by constructing specially crafted ASX files that could potentially allow remote code execution if a user visits a malicious Web site or opens a specially crafted ASX file in an e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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?

The processing code within Windows Media Format Runtime which handles certain URLs included in ASX files.

[NT] Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06-078)

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 is Advanced Stream Redirector (ASX)?

ASX (Advanced Stream Redirector) format is a type of XML metafile designed to store a list of Windows Media files to play during a multimedia presentation. It is used frequently on streaming video servers where multiple ASF files are to be played in succession. Both RTSP and MMS streaming protocols are supported, as well as HTTP. ASX files have MIME type video/x-ms-asf (as do ASF files).

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?

An attacker could host a specially crafted Web site that is designed to exploit these vulnerabilities through Internet Explorer and then persuade a user to view the Web site. This can also include Web sites that accept user-provided content or advertisements, Web sites that host user-provided content or advertisements, and compromised Web sites. These Web sites could contain specially crafted content that could exploit these vulnerabilities. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or in an Instant Messenger message that takes users to the attacker's Web site. It could also be possible to display specially crafted 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.

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers could be at more risk if administrators allow users to log on to servers and to run programs. However, best practices strongly discourage allowing this.

What does the update do?

The update removes the vulnerability by modifying the way that Windows Media Format Runtime validates the length of data in the before passing the data to the allocated buffer.

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

Yes. This vulnerability had been publicly disclosed when this security bulletin was originally issued. It has been assigned the Common Vulnerability and Exposure number CVE-2006-6134.

[NT] Vulnerability in Windows Media Format Could Allow Remote Code Execution (MS06-078)

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 original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS06-078.msp>>
<http://www.microsoft.com/technet/security/Bulletin/MS06-078.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@xxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====
=====

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.