

[NT] Windows Media Player Plug-in for Non-Microsoft Browsers Remote Code Execution (MS06-006)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00050.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2006 11:55:11 +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 Plug-in for Non-Microsoft Browsers Remote Code Execution (MS06-006)

SUMMARY

A malicious EMBED element utilizing a remote code execution in the Windows Media Player plug-in for non-Microsoft Internet browsers could potentially grant an attacker complete control over the attacked system.

DETAILS

Vulnerable Systems:

* Microsoft Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=CCDD3D35-BE5C-4C43-8FFA-BB8570A7321C>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=CCDD3D35-BE5C-4C43-8FFA-BB8570A7321C>>

Download the update

* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

[NT] Windows Media Player Plug-in for Non-Microsoft Browsers Remote Code Execution (MS06-006)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=CCDD3D35-BE5C-4C43-8FFA-BB8570A7321C>>

Download the update

* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=165916C2-037E-4EDD-B64A-84838BEE151C>>

Download the update

* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E3DAAB50-2AC7-49DD-8971-4F98FED9FBA6>>

Download the update

Immune Systems:

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

* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

Mitigating Factors for Windows Media Player Plug-in Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0005>>

CVE-2006-0005:

* Users who use Microsoft Windows Internet Explorer are not vulnerable to this issue.

* 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.

* 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 Plug-in Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0005>>

CVE-2006-0005:

* 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.

* Modify the Access Control List on the Npdsplay.dll file

Modifying the Access Control List on the Npdsplay.dll file helps protect the affected system from attempts to exploit this vulnerability. To modify the Npdsplay.dll file, follow these steps.

1. Click Start then click Run.

2. Type `cacls %programfiles%\Windows Media Player\npdsplay.dll /d everyone`, and then click OK.

[NT] Windows Media Player Plug-in for Non-Microsoft Browsers Remote Code Execution (MS06-006)

Note On x64 platforms use %programfiles(x86)% instead of %programfiles%.

Impact of Workaround: Web sites that attempt to play multimedia content using the non-standard EMBED element may fail to display properly in non-Microsoft Internet browsers. Sites that use the OBJECT element to display content are unaffected by this workaround.

FAQ for Windows Media Player Plug-in Vulnerability –
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0005>>
CVE-2006-0005:

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.

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 impacted than users who operate with administrative user rights.

What causes the vulnerability?

An unchecked buffer in the Windows Media Player plug-in.

What is the Windows Media Player plug-in?

The Windows Media Player plug-in allows users the ability to stream media through a non-Microsoft Internet browser.

Can the Windows Media Player plug-in be used from within Internet Explorer?

No, the Windows Media Player plug-in can only be used from within a non-Microsoft Internet browser such as Netscape Navigator.

What might an attacker use the vulnerability to do?

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

Who could 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.

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers could be

[NT] Windows Media Player Plug-in for Non-Microsoft Browsers Remote Code Execution (MS06-006)

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.

What does the update do?

The update removes the vulnerability by modifying the way that Windows Media Player plug-in 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.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS06-006.msp>>
<http://www.microsoft.com/technet/security/Bulletin/MS06-006.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@xxxxxxxxxxxxxx

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

=====
=====

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.