Abysssec Research

1) Advisory information

Title	: Microsoft Cinepak Codec CVDecompress heap overflow (MS10-055)
Version	: iccvid.dll XP SP3
Analysis	: http://www.abysssec.com
Vendor	: http://www.microsoft.com
Impact	: High
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec
CVE	: CVE-2010-2553

2) Vulnerable version

Microsoft Windows XP Tablet PC Edition SP2
Microsoft Windows XP Professional x64 Edition SP2
Microsoft Windows XP Professional SP3
Microsoft Windows XP Media Center Edition SP3
Microsoft Windows XP Home SP3
Microsoft Windows Vista x64 Edition SP2
Microsoft Windows Vista x64 Edition SP1
Microsoft Windows Vista Ultimate 64-bit edition SP2
Microsoft Windows Vista Ultimate 64-bit edition SP1
Microsoft Windows Vista Home Premium 64-bit edition SP2
Microsoft Windows Vista Home Premium 64-bit edition SP1
Microsoft Windows Vista Home Basic 64-bit edition SP2
Microsoft Windows Vista Home Basic 64-bit edition SP1
Microsoft Windows Vista Enterprise 64-bit edition SP2
Microsoft Windows Vista Enterprise 64-bit edition SP1
Microsoft Windows Vista Business 64-bit edition SP2
Microsoft Windows Vista Business 64-bit edition SP1
Microsoft Windows Vista Ultimate SP2
Microsoft Windows Vista Ultimate SP1
Microsoft Windows Vista SP2
Microsoft Windows Vista SP1
Microsoft Windows Vista Home Premium SP2
Microsoft Windows Vista Home Premium SP1
Microsoft Windows Vista Home Basic SP2
Microsoft Windows Vista Home Basic SP1
Microsoft Windows Vista Enterprise SP2

Microsoft Windows Vista Enterprise SP1
Microsoft Windows Vista Business SP2
Microsoft Windows Vista Business SP1
Microsoft Windows 7 Ultimate 0
Microsoft Windows 7 Starter 0
Microsoft Windows 7 Professional 0
Microsoft Windows 7 Home Premium 0
Microsoft Windows 7 for x64-based Systems 0
Microsoft Windows 7 for Itanium-based Systems 0
Microsoft Windows 7 for 32-bit Systems 0

3) Vulnerability information

Class

1- Heap overflow

Impact

Successfully exploiting this issue allows remote attackers to execute arbitrary code or cause denial-of-service conditions.

Remotely Exploitable

Yes

Locally Exploitable

Yes

4) Vulnerabilities detail

Cinepak(iccvid.dll) is one of the default codec Microsoft support which is used in processing of video files compressed by Cinepak Codec**.**

Streams that is compressed by Cinepak contains a frame header that followed by some strips. Every strips contains CVID data. Number of strip is specified in frame header. For more information about Cinepak stream format refer to the following link:

http://multimedia.cx/mirror/cinepak.txt

CVDecompress function of iccvid.dll module is responsible for decompressing Cinepak streams. In part of the function some value of frame header specifying number of strips

is read and if greater than zero, enters to a loop that strip datas is processing in the loop. Number of iteration is depends on number of strips in a frame. Of course the function considers number of strips is less than 3 but there is no check on this value.

Here is the CVDecompress function of iccvid.dll module.

```
.text:73C02221          xor     eax, eax
.text:73C02223          mov     ah, [esi+8]
.text:73C02226          add     esi, 0Ah
.text:73C02229          mov     [ebp+var_14], edi
.text:73C0222C          mov     [ebp+var_18], esi
.text:73C0222F          mov     [ebp+var_C], esi
.text:73C02232          mov     al, [esi-1]
.text:73C02235          cmp     eax, edi
.text:73C02237          mov     [ebp+var_1C], eax
.text:73C0223A          jle     loc_73C023EA
.text:73C02240          mov     [ebp+var_4], edi
```

In the beginning of this loop length of the unprocessed Cinepack stream is compared with 0x16 and if greater, processing of the next strip is performed. Of course in next stage this value is compared with the length of current strip which in case of greater value continue processing from that strip.

```
.text:73C02243          mov     eax, [ebp+var_10]
.text:73C02246          cmp     eax, 16h
.text:73C02249          jb      loc_73C023EA
.text:73C0224F          movzx   edx, byte ptr [esi+3]
.text:73C02253          xor     ecx, ecx
.text:73C02255          mov     ch, [esi+1]
.text:73C02258          mov     cl, [esi+2]
.text:73C0225B          shl     ecx, 8
.text:73C0225E          or      ecx, edx
.text:73C02260          cmp     eax, ecx
.text:73C02262          mov     [ebp+var_8], ecx
```

Then some variable is checked that this variable is incremented by 0x2000 in each iteration of the loop. In the first iteration this value is equal to zero but incremented by 0x2000 in next iterations. Now if this variable greater than zero and also value of ID of the stream equal to 0x1100, our data will be copied to a heap buffer with a fix size and by each iteration of the loop and the mentioned conditions, the pointer to buffer is incremented by 0x2000.

```
.text:73C022A9          mov     eax, [ebp+var_4]
```

```
.text:73C022AC          cmp     eax, edi
.text:73C022AE          jz      short loc_73C022D1
.text:73C022B0          cmp     byte ptr [ebp+arg_8+3], 0
.text:73C022B4          jnz     short loc_73C022D1
.text:73C022B6          cmp     byte ptr [esi], 11h
.text:73C022B9          jnz     short loc_73C022D1
.text:73C022BB          mov     ecx, [ebx+1Ch]
.text:73C022BE          lea     edi, [ecx+eax]
.text:73C022C1          mov     ecx, 800h
.text:73C022C6          lea     esi, [edi-2000h]
.text:73C022CC          rep movsd
.text:73C022CE          mov     esi, [ebp+var_18]

...

.text:73C023B9          movsx   eax, word ptr [ebp+arg_4]
.text:73C023BD          imul    eax, [ebp+arg_18]
.text:73C023C1          add     [ebp+arg_14], eax
.text:73C023C4          inc     [ebp+var_14]
.text:73C023C7          add     [ebp+var_4], 2000h
.text:73C023CE          xor     edi, edi
```

Now if value of number of strips in the frame header is greater than 3, and in each iteration of strips processing length of the unprocessed Cinepack stream is greater than 0x16, our data causes a heap overflow in copying process.

Check out PoC here: link to Poc