MOAUB

Abysssec Research

1) Advisory information

Title	:	Microsoft Excel HFPicture Record Parsing Remote Code Execution Vulnerability
Version	:	Excel 2002 SP3
Analysis	:	http://www.abysssec.com
Vendor	:	http://www.microsoft.com
Impact	:	Med/High
Contact	:	shahin [at] abysssec.com , info [at] abysssec.com
Twitter	:	@abysssec
CVE	:	CVE-2010-1248

2) Vulnerable version

Microsoft Office 2004 for Mac 0
Microsoft Excel 2002 SP3
+ Microsoft Office XP SP3
Microsoft Excel 2002 SP2
+ Microsoft Office XP SP2
- Microsoft Windows 2000 Professional SP3
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional
- Microsoft Windows 98
- Microsoft Windows 98SE
- Microsoft Windows ME
- Microsoft Windows NT Workstation 4.0 SP6a
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP1

```
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows XP Home SP1
- Microsoft Windows XP Home
- Microsoft Windows XP Professional SP1
- Microsoft Windows XP Professional
Microsoft Excel 2002 SP1
+ Microsoft Office XP SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Terminal Services SP2
- Microsoft Windows 2000 Terminal Services SP1
- Microsoft Windows 2000 Terminal Services
- Microsoft Windows 98
- Microsoft Windows 98SE
- Microsoft Windows ME
- Microsoft Windows NT Enterprise Server 4.0 SP6a
- Microsoft Windows NT Enterprise Server 4.0 SP6
- Microsoft Windows NT Enterprise Server 4.0 SP5
- Microsoft Windows NT Enterprise Server 4.0 SP4
- Microsoft Windows NT Enterprise Server 4.0 SP3
- Microsoft Windows NT Enterprise Server 4.0 SP2
- Microsoft Windows NT Enterprise Server 4.0 SP1
- Microsoft Windows NT Enterprise Server 4.0
- Microsoft Windows NT Server 4.0 SP6a
- Microsoft Windows NT Server 4.0 SP6
- Microsoft Windows NT Server 4.0 SP5
- Microsoft Windows NT Server 4.0 SP4
- Microsoft Windows NT Server 4.0 SP3
- Microsoft Windows NT Server 4.0 SP2
- Microsoft Windows NT Server 4.0 SP1
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Terminal Server 4.0 SP6
- Microsoft Windows NT Terminal Server 4.0 SP5
- Microsoft Windows NT Terminal Server 4.0 SP4
- Microsoft Windows NT Terminal Server 4.0 SP3
- Microsoft Windows NT Terminal Server 4.0 SP2
- Microsoft Windows NT Terminal Server 4.0 SP1
- Microsoft Windows NT Terminal Server 4.0
```

- Microsoft Windows NT Workstation 4.0 SP6a
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP1
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows XP Home
- Microsoft Windows XP Professional

Microsoft Excel 2002
+ Microsoft Office XP

- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional
- Microsoft Windows 95 SR2
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows 98SE
- Microsoft Windows ME
- Microsoft Windows NT 4.0 SP6a
- Microsoft Windows NT 4.0 SP5
- Microsoft Windows NT 4.0 SP4
- Microsoft Windows NT 4.0 SP3
- Microsoft Windows NT 4.0 SP2
- Microsoft Windows NT 4.0 SP1
- Microsoft Windows NT 4.0

Avaya Messaging Application Server MM 3.1
Avaya Messaging Application Server MM 3.0
Avaya Messaging Application Server MM 2.0
Avaya Messaging Application Server MM 1.1
Avaya Messaging Application Server 5
Avaya Messaging Application Server 4
Avaya Messaging Application Server 0
Avaya Meeting Exchange - Webportal 0
Avaya Meeting Exchange - Web Conferencing Server 0
Avaya Meeting Exchange - Streaming Server 0
Avaya Meeting Exchange - Recording Server 0
Avaya Meeting Exchange - Client Registration Server 0

3) Vulnerability information

Class

1- Buffer overflow

Impact

Attackers can exploit this issue by enticing an unsuspecting user to open a specially crafted Excel ('.xls') file. Successful exploits can allow attackers to execute arbitrary code with the privileges of the user running the application.

Remotely Exploitable

Yes

Locally Exploitable

Yes

4) Vulnerabilities detail

HFPicture record consists of an integrated encryption of a picture contents that may be a MSODRAWING or MSODRAWINGGROUP record format. The fields of this record consist of the followings:

Offset	**Name**	**Size**	**Contents**
4	rt	2	Record type; this matches the BIFF rt in the first two bytes of the record; =0866h
6	grbitFrt	2	FRT flags; must be zero
8	(unused)	8	Must be zero
16	rgf	1	Bit flags, see description below.

5	rgb	var	An embedded encoding of the contents of the picture; May be in MSODRAWING or MSODRAWINGGROUP record format as indicated in rgf flags listed below.

The sub_3057124E function is responsible for processing this record. rgb field is used for encryption. One of the functions called in the process of rgb is sub_30E2AFAF from mso.dll module:

```
.text:30E2AFD0              lea     eax, [ebp+arg_0]
.text:30E2AFD3              mov     ecx, edi
.text:30E2AFD5              push    eax
.text:30E2AFD6              call    sub_30E2B01F
.text:30E2AFDB              test    eax, eax
.text:30E2AFDD              jz      loc_30F094DF
.text:30E2AFE3              cmp     [ebp+var_4], 4
.text:30E2AFE7              jge     short loc_30E2B002
.text:30E2AFE9              mov     eax, [ebp+arg_0]
.text:30E2AFEC              mov     ecx, ebx
.text:30E2AFEE              mov     [ebp+var_8], eax
.text:30E2AFF1              call    sub_30B41399
.text:30E2AFF6              mov     ecx, ebx
.text:30E2AFF8              call    sub_30B4144A
.text:30E2AFFD              mov     eax, [ebp+var_8]
.text:30E2B000              mov     [ebx], eax
.text:30E2B002
.text:30E2B002 loc_30E2B002:                        ; CODE XREF: sub_30E2AFAF+38j
.text:30E2B002              mov     eax, [edi+14h]   → خواندن چهار بایت از فیلد rgb
.text:30E2B005              inc     [ebp+var_4]
.text:30E2B008              shr     eax, 4
.text:30E2B00B              and     eax, esi
.text:30E2B00D              add     ebx, 18h
.text:30E2B010              cmp     [ebp+var_4], eax
.text:30E2B013              jl      short loc_30E2AFD0
```

In the above function 4bytes of values from this field is read and the result of shifting it 4bytes right and logic 'and' with 0FFF value will be compared with some number and if greater than that the execution is moved to the beginning of the loop causing sub_30E2B01F to be called.

Now it can be considered vulnerable because there is no control on the value of the 4byte read rgb.

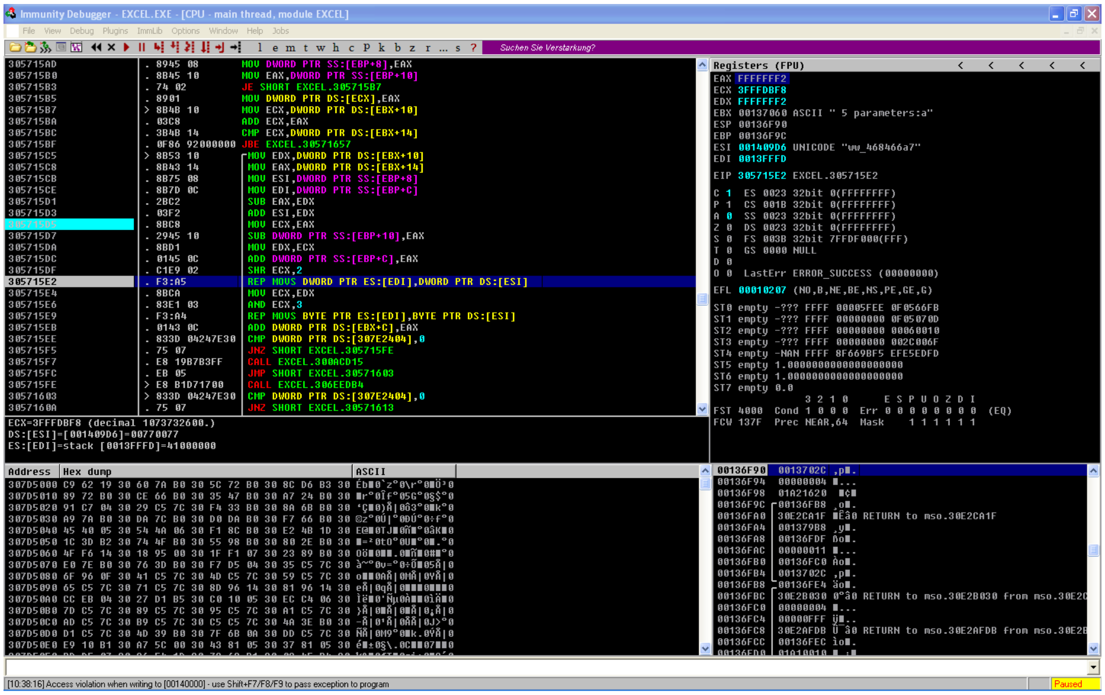
If follow the sub_30E2B01F function, you stop at the sub_57159C function:

```
.text:3057159C              push    ebp
.text:3057159D              mov     ebp, esp
.text:305715B7              mov     ecx, [ebx+10h]
.text:305715BA              add     ecx, eax
.text:305715BC              cmp     ecx, [ebx+14h]
.text:305715BF              jbe     loc_30571657
.text:305715C5
.text:305715C5 loc_305715C5:                        ; CODE XREF: sub_3057159C+B2j
.text:305715C5              mov     edx, [ebx+10h]
```

```
.text:305715C8          mov     eax, [ebx+14h]
.text:305715CB          mov     esi, [ebp+arg_0]
.text:305715CE          mov     edi, [ebp+arg_4]
.text:305715D1          sub     eax, edx
.text:305715D3          add     esi, edx
.text:305715D5          mov     ecx, eax
.text:305715D7          sub     [ebp+arg_8], eax
.text:305715DA          mov     edx, ecx
.text:305715DC          add     [ebp+arg_4], eax
.text:305715DF          shr     ecx, 2
.text:305715E2          rep movsd
.text:305715E4          mov     ecx, edx
.text:305715E6          and     ecx, 3
.text:305715E9          rep movsb
.text:305715EB          add     [ebx+0Ch], eax
.text:305715EE          cmp     dword_3080A110, 0
.text:305715F5          jnz     short loc_305715FE
.text:305715F7          call    sub_300ACD15
.text:305715FC          jmp     short loc_30571603
```

This function copies the content of records related to encryption in some buffer. In part of the function it checks whether we reach the end of the record or not. In case of the end of the record the length of the next record will be substitute by constant value of 0Eh. An then according to the result the buffer copying operation will be performed.

The main problem of this vulnerability is not checking the result of the substitution. If the length of the next record is less than the 0Eh the result is a negative or on the other way a very big number. So with the amount of this big number will be copied to the buffer.


Immunity Debugger - EXCEL.EXE - [CPU - main thread, module EXCEL]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Suchen Sie Verstarkung?
Registers (FPU)
Address
Hex dump
ASCII
Paused

```
305715AD  . 8945 08         MOV DWORD PTR SS:[EBP+8],EAX
305715B0  . 8B45 10         MOV EAX,DWORD PTR SS:[EBP+10]
305715B3  . 74 02           JE SHORT EXCEL.305715B7
305715B5  . 8901            MOV DWORD PTR DS:[ECX],EAX
305715B7  > 8B4B 10         MOV ECX,DWORD PTR DS:[EBX+10]
305715BA  . 03C8            ADD ECX,EAX
305715BC  . 3B4B 14         CMP ECX,DWORD PTR DS:[EBX+14]
305715BF  . 0F86 92000000   JBE EXCEL.30571657
305715C5  > 8B53 10         MOV EDX,DWORD PTR DS:[EBX+10]
305715C8  . 8B43 14         MOV EAX,DWORD PTR DS:[EBX+14]
305715CB  . 8B75 08         MOV ESI,DWORD PTR SS:[EBP+8]
305715CE  . 8B7D 0C         MOV EDI,DWORD PTR SS:[EBP+C]
305715D1  . 2BC2            SUB EAX,EDX
305715D3  . 03F2            ADD ESI,EDX
305715D5  . 8BC8            MOV ECX,EAX
305715D7  . 2945 10         SUB DWORD PTR SS:[EBP+10],EAX
305715DA  . 8BD1            MOV EDX,ECX
305715DC  . 0145 0C         ADD DWORD PTR SS:[EBP+C],EAX
305715DF  . C1E9 02         SHR ECX,2
305715E2  . F3:A5           REP MOVS DWORD PTR ES:[EDI],DWORD PTR DS:[ESI]
305715E4  . 8BCA            MOV ECX,EDX
305715E6  . 83E1 03         AND ECX,3
305715E9  . F3:A4           REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
305715EB  . 0143 0C         ADD DWORD PTR DS:[EBX+C],EAX
305715EE  . 833D 04247E30   CMP DWORD PTR DS:[307E2404],0
305715F5  . 75 07           JNZ SHORT EXCEL.305715FE
305715F7  . E8 19B7B3FF     CALL EXCEL.300ACD15
305715FC  . EB 05           JMP SHORT EXCEL.30571603
305715FE  > E8 B1D71700     CALL EXCEL.306EEDB4
30571603  > 833D 04247E30   CMP DWORD PTR DS:[307E2404],0
3057160A  . 75 07           JNZ SHORT EXCEL.30571613
ECX=3FFFDBF8 (decimal 1073732600.)
DS:[ESI]=[001409D6]=00770077
ES:[EDI]=stack [0013FFFD]=41000000
```

```
EAX FFFFFFF2
ECX 3FFFDBF8
EDX FFFFFFF2
EBX 00137060 ASCII " 5 parameters:a"
ESP 00136F90
EBP 00136F9C
ESI 001409D6 UNICODE "ww_468466a7"
EDI 0013FFFD

EIP 305715E2 EXCEL.305715E2

C 1  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010207 (NO,B,NE,BE,NS,PE,GE,G)

ST0 empty -??? FFFF 00005FEE 0F0566FB
ST1 empty -??? FFFF 00000000 0F05070D
ST2 empty -??? FFFF 00000000 00060010
ST3 empty -??? FFFF 00000000 002C006F
ST4 empty -NAN FFFF 8F669BF5 EFE5EDFD
ST5 empty 1.0000000000000000000
ST6 empty 1.0000000000000000000
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 4000  Cond 1 0 0 0  Err 0 0 0 0 0 0 0 0  (EQ)
FCW 137F  Prec NEAR,64  Mask    1 1 1 1 1 1
```

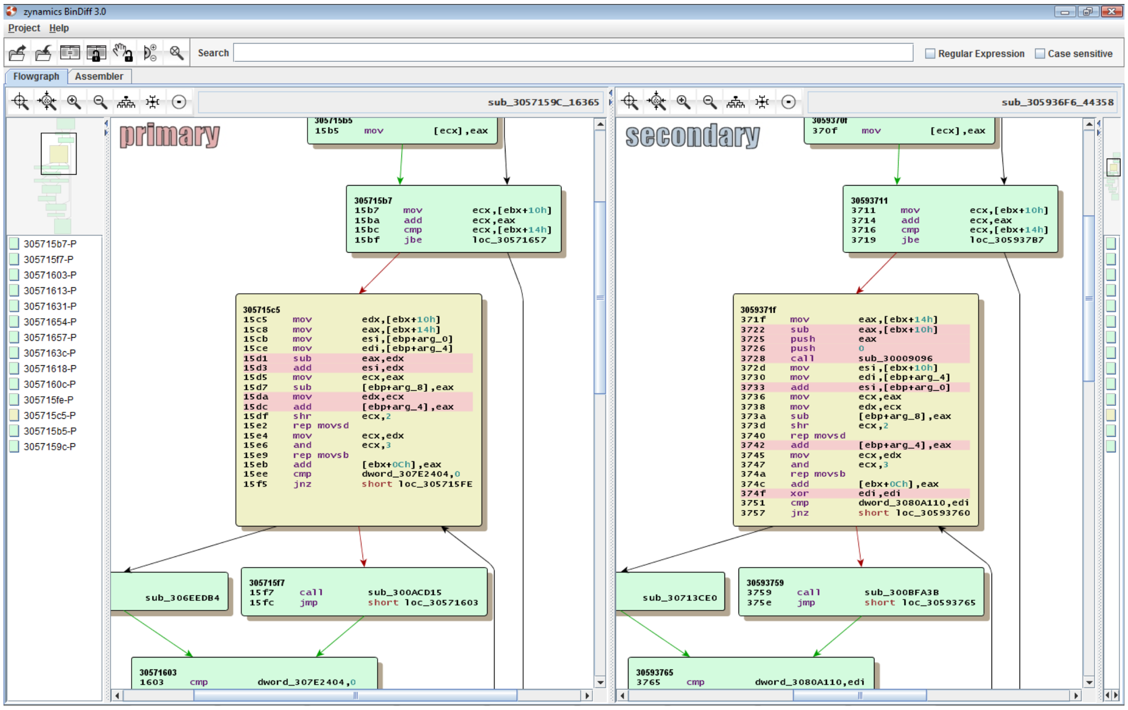
```
Address  Hex dump                                         ASCII
307D5000 C9 62 19 30 60 7A B0 30 5C 72 B0 30 8C D6 B3 30 Éb■0`z°0\r°0■Ö³0
307D5010 89 72 B0 30 CE 66 B0 30 35 47 B0 30 A7 24 B0 30 ■r°0Îf°05G°0§$°0
307D5020 91 C7 04 30 29 C5 7C 30 F4 33 B0 30 8A 6B B0 30 ‘Ç■0)Å|0ô3°0■k°0
307D5030 A9 7A B0 30 DA 7C B0 30 D0 DA B0 30 F7 66 B0 30 ©z°0Ú|°0ÐÚ°0÷f°0
307D5040 45 40 05 30 54 4A 06 30 F1 8C B0 30 E2 4B 1D 30 E@■0TJ■0ñ■°0âK■0
307D5050 1C 3D B2 30 74 4F B0 30 55 98 B0 30 80 2E B0 30 ■=²0tO°0U■°0■.°0
307D5060 4F F6 14 30 18 95 00 30 1F F1 07 30 23 89 B0 30 Oö■0■■.0■ñ■0#■°0
307D5070 E0 7E B0 30 76 3D B0 30 F7 D5 04 30 35 C5 7C 30 à~°0v=°0÷Õ■05Å|0
307D5080 6F 96 0F 30 41 C5 7C 30 4D C5 7C 30 59 C5 7C 30 o■■0AÅ|0MÅ|0YÅ|0
307D5090 65 C5 7C 30 71 C5 7C 30 8D 96 14 30 81 96 14 30 eÅ|0qÅ|0■■■0■■■0
307D50A0 CC EB 04 30 27 D1 B5 30 C0 10 05 30 EC C4 06 30 Ìë■0'Ñµ0À■■0ìÄ■0
307D50B0 7D C5 7C 30 89 C5 7C 30 95 C5 7C 30 A1 C5 7C 30 }Å|0■Å|0■Å|0¡Å|0
307D50C0 AD C5 7C 30 B9 C5 7C 30 C5 C5 7C 30 4A 3E B0 30 -Å|0¹Å|0ÅÅ|0J>°0
307D50D0 D1 C5 7C 30 4D 39 B0 30 7F 6B 0A 30 DD C5 7C 30 ÑÅ|0M9°0■k.0ÝÅ|0
307D50E0 E9 10 B1 30 A7 5C 00 30 43 81 05 30 37 81 05 30 é■±0§\.0C■■07■■0
```

```
00136F90   0013702C ,p■.
00136F94   00000004 ■...
00136F98   01A21620  ■¢■
00136F9C  ┌00136FB8 ¸o■.
00136FA0  │30E2CA1F ■Êâ0 RETURN to mso.30E2CA1F
00136FA4  │001379B8 ¸y■.
00136FA8  │00136FDF ßo■.
00136FAC  │00000011 ■...
00136FB0  │00136FC0 Ào■.
00136FB4  │0013702C ,p■.
00136FB8  └00136FE4 äo■.
00136FBC  ┌30E2B030 0°â0 RETURN to mso.30E2B030 from mso.30E2C
00136FC0  │00000004 ■...
00136FC4  │00000FFF ÿ■..
00136FC8  │30E2AFDB Û¯â0 RETURN to mso.30E2AFDB from mso.30E2B
00136FCC  │00136FEC ìo■.
```

[10:38:16] Access violation when writing to [00140000] - use Shift+F7/F8/F9 to pass exception to program

In order to crash the program 58bytes from the beginning of the record should be skipped, then initializing with 4byte will crash the program depend on your value. For finding the beginning of this record in the poc file search the '66 08 4E 00' value in the hex editor (Be care that the 866 value is the identity for HFPicture record)

In the following graph you can see the comparison between vulnerable and patched code relating to the XP sp3. As you see in the patched version some checking code is added to the function for the substitution.



```
305715b5
15b5     mov      [ecx],eax

305715b7
15b7     mov      ecx,[ebx+10h]
15ba     add      ecx,eax
15bc     cmp      ecx,[ebx+14h]
15bf     jbe      loc_30571657

305715c5
15c5     mov      edx,[ebx+10h]
15c8     mov      eax,[ebx+14h]
15cb     mov      esi,[ebp+arg_0]
15ce     mov      edi,[ebp+arg_4]
15d1     sub      eax,edx
15d3     add      esi,edx
15d5     mov      ecx,eax
15d7     sub      [ebp+arg_8],eax
15da     mov      edx,ecx
15dc     add      [ebp+arg_4],eax
15df     shr      ecx,2
15e2     rep movsd
15e4     mov      ecx,edx
15e6     and      ecx,3
15e9     rep movsb
15eb     add      [ebx+0Ch],eax
15ee     cmp      dword_307E2404,0
15f5     jnz      short loc_305715FE

         sub_306EEDB4

305715f7
15f7     call     sub_300ACD15
15fc     jmp      short loc_30571603

30571603
1603     cmp      dword_307E2404,0
```

```
3059370f
370f     mov      [ecx],eax

30593711
3711     mov      ecx,[ebx+10h]
3714     add      ecx,eax
3716     cmp      ecx,[ebx+14h]
3719     jbe      loc_305937B7

3059371f
371f     mov      eax,[ebx+14h]
3722     sub      eax,[ebx+10h]
3725     push     eax
3726     push     0
3728     call     sub_30009096
372d     mov      esi,[ebx+10h]
3730     mov      edi,[ebp+arg_4]
3733     add      esi,[ebp+arg_0]
3736     mov      ecx,eax
3738     mov      edx,ecx
373a     sub      [ebp+arg_8],eax
373d     shr      ecx,2
3740     rep movsd
3742     add      [ebp+arg_4],eax
3745     mov      ecx,edx
3747     and      ecx,3
374a     rep movsb
374c     add      [ebx+0Ch],eax
374f     xor      edi,edi
3751     cmp      dword_3080A110,edi
3757     jnz      short loc_30593760

         sub_30713CE0

30593759
3759     call     sub_300BFA3B
375e     jmp      short loc_30593765

30593765
3765     cmp      dword_3080A110,edi
```

EXPLOIT

As we discussed earlier the vulnerability can be stack overflow. Demonstrated on above picture all of the stack are overwritten, so the seh structure overwritten too. If someone able to gain the values of this structure can exploit the vulnerability.