

Currently archiving 12671 exploits

Archive last Updated: Sun Sep 12 2010

- [Home](#)
- [Blog](#)
- [About](#)
- [Remote](#)
- [Local](#)
- [Web](#)
- [DoS](#)
- [Shellcode](#)
- [Papers](#)
- [Search](#)
- [Submit](#)
- [Archive](#)



MAOUB #16 – Microsoft Excel HFPicture Record Parsing Remote Code Execution Vulnerability

16th September 2010 - by admin



Abysssec Research

1) Advisory information

Title	Microsoft Excel HFPicture Record Parsing Remote Code Execution Vulnerability
Version	Excel 2002 SP3
Analysis	http://www.abyssec.com
Vendor	http://www.microsoft.com
Impact	Med/High
Contact	shahin [at] abyssec.com , info [at] abyssec.com
Twitter	@abyssec
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_30E2AF4F from mso.dll module:

```

1 .text:30E2AFD0      lea  eax, [ebp+arg_0]
2 .text:30E2AFD3      mov  ecx, edi
3 .text:30E2AFD5      push eax
4 .text:30E2AFD6      call sub_30E2B01F
5 .text:30E2AFDB      test eax, eax
6 .text:30E2AFDD      jz   loc_30F094DF
7 .text:30E2AFE3      cmp  [ebp+var_4], 4
8 .text:30E2AFE7      jge  short loc_30E2B002
9 .text:30E2AFE9      mov  eax, [ebp+arg_0]
10 .text:30E2AFEC     mov  ecx, ebx
11 .text:30E2AFEE     mov  [ebp+var_8], eax
12 .text:30E2AFF1     call sub_30B41399
13 .text:30E2AFF6     mov  ecx, ebx
14 .text:30E2AFF8     call sub_30B4144A
15 .text:30E2AFFD     mov  eax, [ebp+var_8]
16 .text:30E2B000     mov  [ebx], eax

```

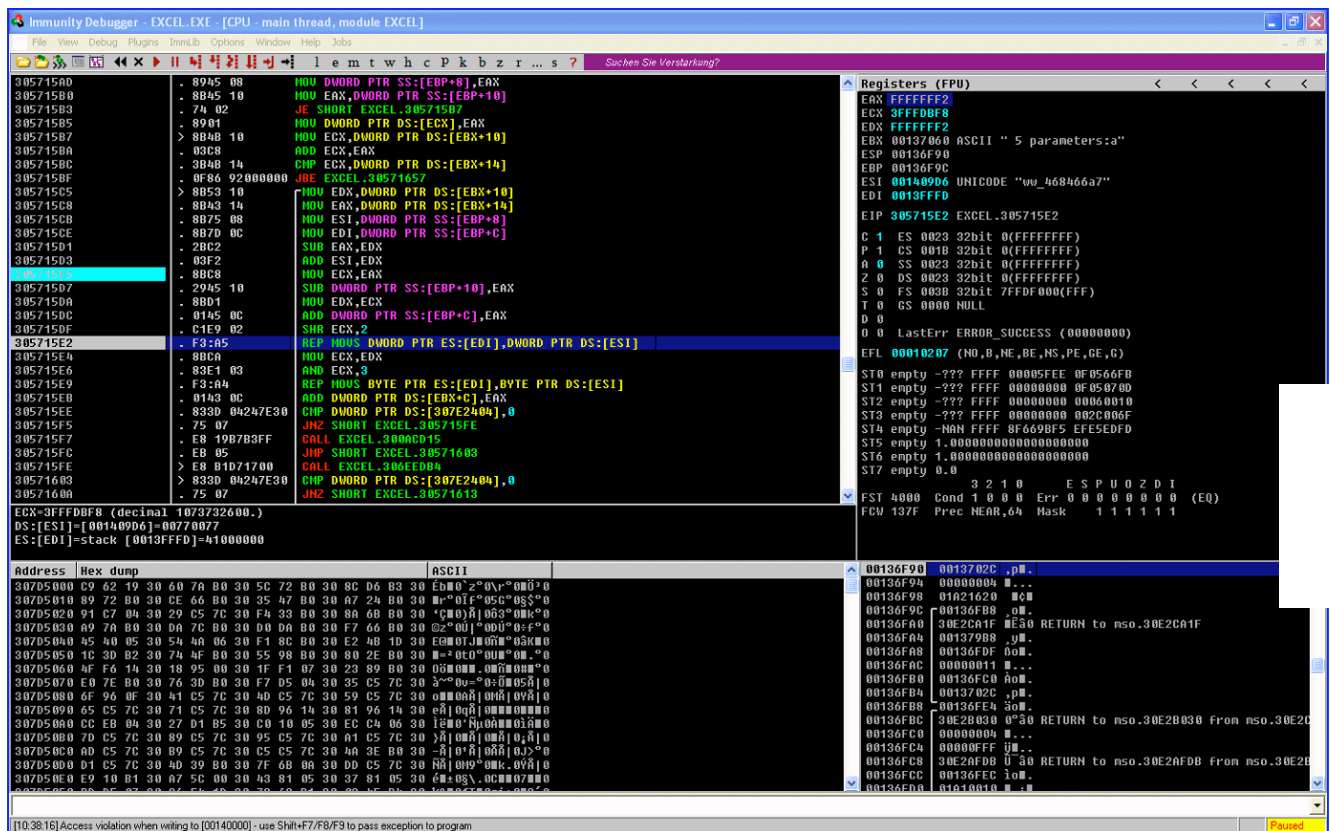
In the above function 4bytes of values from this field is read and the result of shifting it 4bytes right and logic 'and' with 0FFF value will be compared with some number and if greater than that the execution is moved to the beginning of the loop causing sub_30E2B01F to be called.

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:

```
1 .text:3057159C      push  ebp
2 .text:3057159D      mov   ebp, esp
3 .text:305715B7      mov   ecx, [ebx+10h]
4 .text:305715BA      add   ecx, eax
5 .text:305715BC      cmp   ecx, [ebx+14h]
6 .text:305715BF      jbe   loc_30571657
7 .text:305715C5
8 .text:305715C5 loc_305715C5:      ; CODE XREF: sub_3057159C+B2j
9 .text:305715C5      mov   edx, [ebx+10h]
10.text:305715C8      mov   eax, [ebx+14h]
11.text:305715CB      mov   esi, [ebp+arg_0]
12.text:305715CE      mov   edi, [ebp+arg_4]
13.text:305715D1      sub   eax, edx
14.text:305715D3      add   esi, edx
15.text:305715D5      mov   ecx, eax
16.text:305715D7      sub   [ebp+arg_8], eax
```

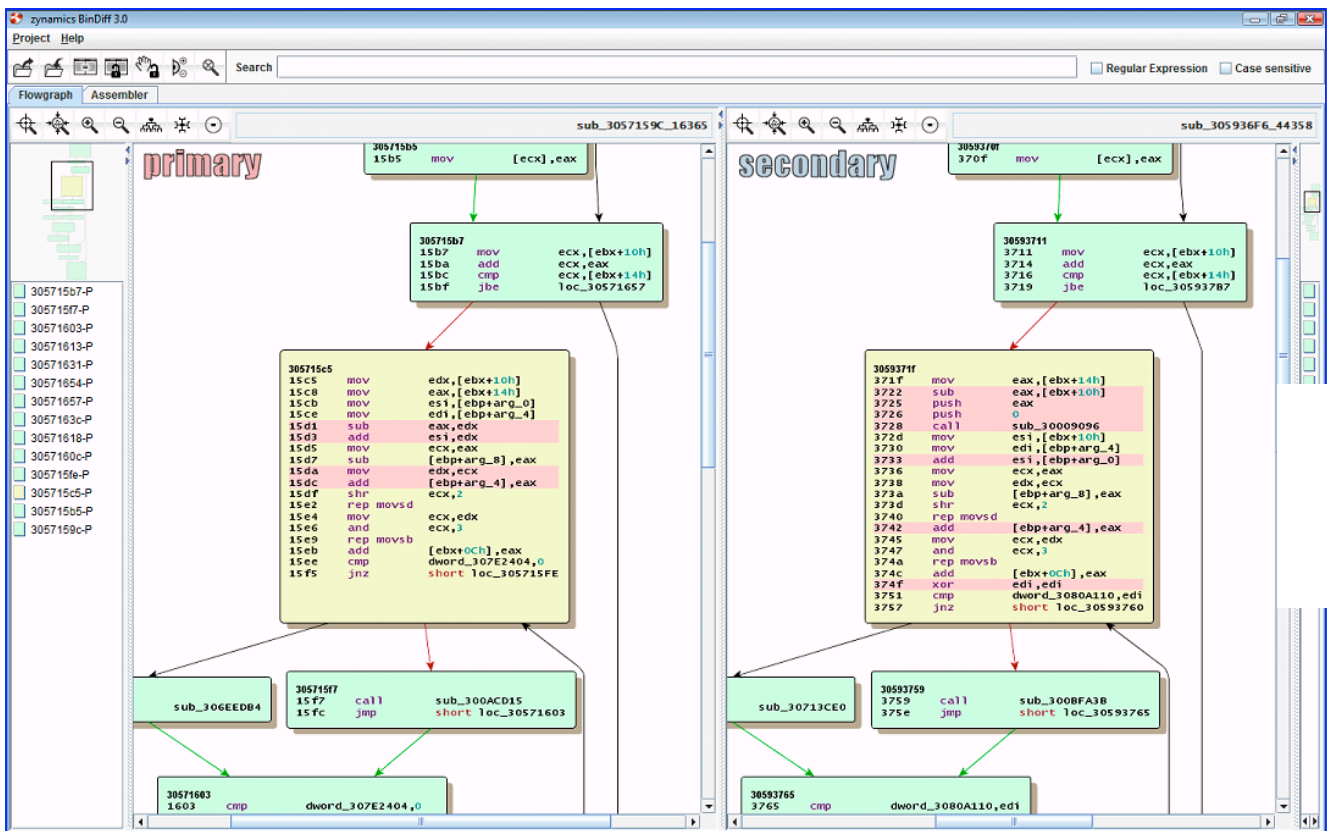
This function copies the content of records related to encryption in some buffer. In part of the function it checks whether we reach the end of the record or not. In case of the end of the record the length of the next record will be substitute by constant value of 0Eh. An then according to the result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



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.



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.

Check out the [Microsoft Excel HFPicture Record Parsing Remote Code Execution Vulnerability PoC](#).

Comments are closed.

© Offensive Security 2010