Abysssec Research

1) Advisory information

Title	: Microsoft Excel WOPT Record Parsing Heap Memory Corruption
Version	: Office Excel 2002(office xp)
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-2010-0824

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- Heap Memory Corruption

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

WOPT record contain settings that we have set in Web Option window. Here is the fields of this record:

Offset	Name	Size	Contents
4	rt	2	Record type; this matches the BIFF rt in the first two bytes of the record; =080Bh
6	grbitFrt	2	FRT flags; must be zero
8	grbit	2	Options; see following table
10	bScreenSize	1	Target monitor screen size 0= 544x376 1= 640x480 2= 720x512 3= 800x600 4= 1024x768 5= 1152x882 6= 1152x900 7= 1280x1024 8= 1600x1200 9= 1800x1440 10= 1920x1200
11	dwPixelsPerInch	4	Target monitor pixels per inch
15	uiCodePage	4	Code page index value
19	cchLocationOfComponents	2	length of the string in rgbLocationOfComponents

21	rgbLocationOfComponents	var	Unicode string; the path to the location for download of the Microsoft Office Web Components
var	rgbFuture	var	Space reserved for bytes from future versions of Excel

The sub_3015C307 function responsible for processing this record:

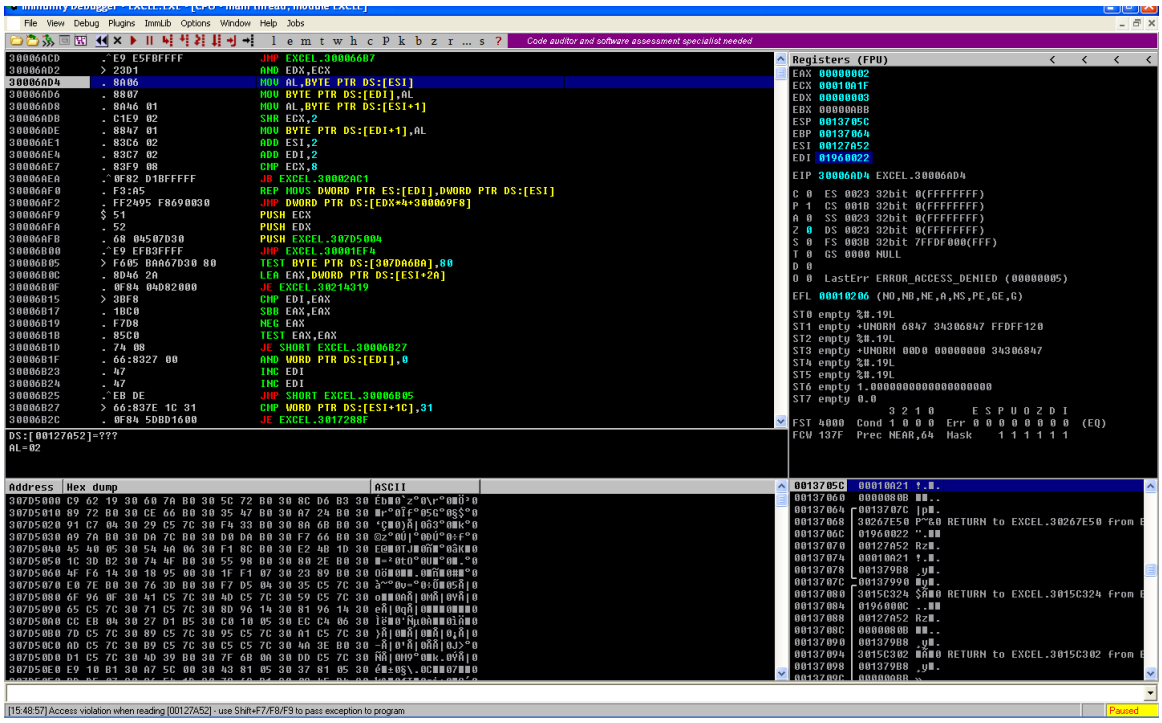
```
.text:3015C307          push    esi
.text:3015C308          mov     esi, [esp+4+arg_0]
.text:3015C30C          mov     ecx, esi
.text:3015C30E          push    edi
.text:3015C30F          movsx   eax, word ptr [esi+10h]
.text:3015C313          lea     eax, [esi+eax*2+12h]
.text:3015C317          sub     ecx, eax
.text:3015C319          push    eax
.text:3015C31A          add     ecx, [esp+0Ch+arg_4]
.text:3015C31E          push    ecx
.text:3015C31F          call    sub_300A197A
```

At the beginning of the function the value of the cchLocationOfComponents is read and then after some calculation on the value it is passed to the sub_300A197A function. 24 is added to this value in the function and based on the result a block of memory is allocated. By calling the sub_300A19AD a block of memory is allocated.

```
.text:300A197E          mov     esi, [ebp+arg_0]
.text:300A1981          push    0
.text:300A1983          push    1020h
.text:300A1988          lea     eax, [esi+18h]
.text:300A198B          push    eax
.text:300A198C          lea     eax, [ebp+arg_0]
.text:300A198F          push    eax
.text:300A1990        call    sub_300A19AD
.text:300A1995          test    eax, eax
.text:300A1997          jz      loc_30267E58
.text:300A199D          test    esi, esi
.text:300A199F          jg      loc_30267E39
...
.text:30267E39          mov     eax, [ebp+arg_0]
.text:30267E3C          push    esi
.text:30267E3D          push    [ebp+arg_4]
.text:30267E40          mov     [eax+14h], si
.text:30267E44          mov     eax, [ebp+arg_0]
.text:30267E47          add     eax, 16h
.text:30267E4A          push    eax
.text:30267E4B        call    sub_30002A8A
```

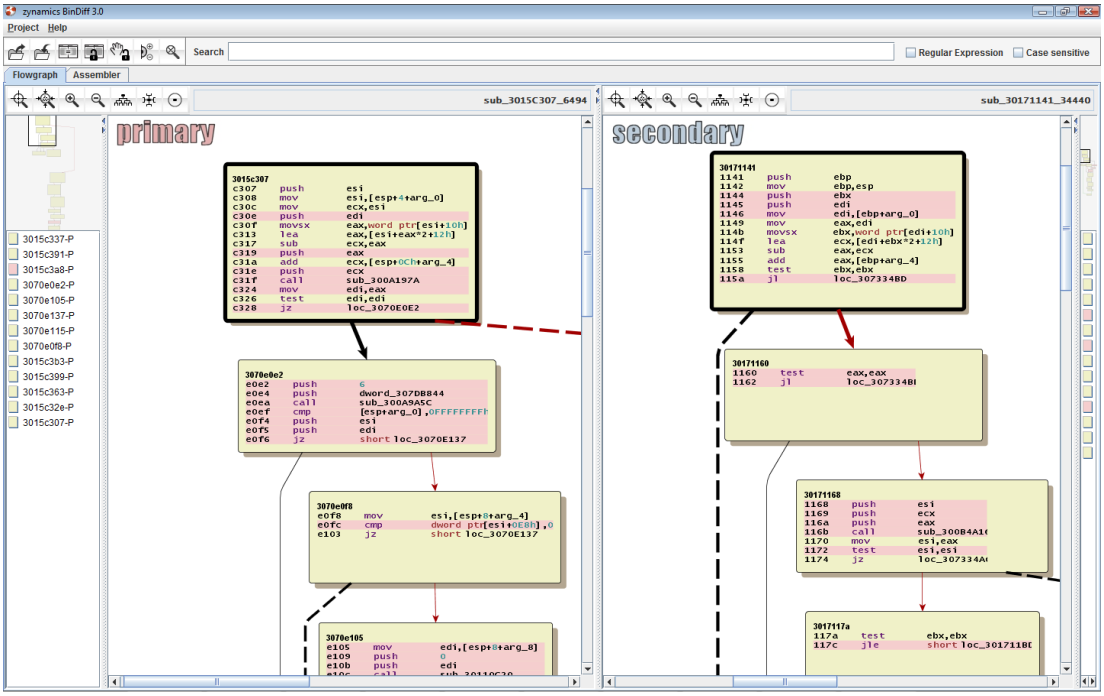
After that sub_30002A8A is called, it copies some values with exact length to a buffer. This function takes 3 arguments. The first argument is a pointer to a buffer. Second one is a pointer to a source. And the last one is the length of bytes should be copied.

If you pay enough care, you can see that the value of the second argument which means pointer to the source is under the control. It means that with the values that we initialize to the cchLocationOfComponents field, this address can be manipulated. If the address is invalid we face an access violation in the sub_30002A8A function.



In order to crash you should skip 20 bytes from the beginning of this record and then initialize 2bytes and the program crash based on your input. To find the beginning of this record in the poc file you should search '0B 08 22 00' in the hex editor. (80b is the identity of the WOPT record)

In the following graphs you see a comparison between the vulnerable code and the patched code. As you see some codes are added to check cchLocationOfComponents field values.



Exploit

It may be possible by manipulating values that is copied to the buffer some other processing code may be affected and by the way being exploitable.