Abysssec Research

1) Advisory information

Title	: Microsoft Excel SxView Record Parsing Memory Corruption
Version	: Excel 2002 SP3
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-2010-1245

2) Vulnerable version

Microsoft Open XML File Format Converter for Mac 0
Microsoft Office 2008 for Mac 0
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- Code execution

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

SXView record consists of high level information of PivotTable. Fields of the record are as follow:

Offset	Name	Size	Contents
4	rwFirst	2	First row of the PivotTable
6	rwLast	2	Last row of the PivotTable
8	colFirst	2	First column of the PivotTable
10	colLast	2	Last column of the PivotTable
12	rwFirstHead	2	First row containing PivotTable headings
14	rwFirstData	2	First row containing PivotTable data
16	colFirstData	2	First column containing PivotTable data
18	iCache	2	Index to the cache
20	(Reserved)	2	Reserved; must be 0 (zero)
22	sxaxis4Data	2	Default axis for a data field
24	ipos4Data	2	Default position for a data field
26	cDim	2	Number of fields
28	cDimRw	2	Number of row fields
30	cDimCol	2	Number of column fields
32	cDimPg	2	Number of page fields
34	cDimData	2	Number of data fields

36	cRw	2	Number of data rows
38	cCol	2	Number of data columns
40	grbit	2	Option flags
42	itblAutoFmt	2	Index to the PivotTable autoformat
44	cchName	2	Length of the PivotTable name
46	cchData	2	Length of the data field name
48	rgch	var	PivotTable name, followed by the name of a data field

sub_3016237B function responsible for the processing of this record. When the processing reach the iCache field sub_3012F2EF function is called:

```
.text:30162625              mov     eax, [esi+68h]
.text:30162628              mov     eax, [eax+8Ch]
.text:3016262E              mov     eax, [eax+214h]
.text:30162634              cmp     [eax+2], di
.text:30162638              jz      loc_30276072
.text:3016263E              push    esi
.text:3016263F              call    sub_3012F2EF
.text:30162644              inc     dword ptr [eax]
.text:30162646              push    esi
.text:30162647              call    sub_3012F2EF
.text:3016264C              add     eax, 0BCh
.text:30162651              and     byte ptr [eax], 7Fh
.text:30162654              mov     eax, [ebp+var_14]
```

sub_3012F2EF function only takes an argument and that is a pointer to a buffer containing SXView record.

Look at the code of this function:

```
.text:3012F2EF              mov     eax, dword_307E15A0
.text:3012F2F4              mov     ecx, [esp+arg_0]
.text:3012F2F8              test    eax, eax
.text:3012F2FA              jnz     loc_30275D14
.text:3012F300
.text:3012F300 loc_3012F300:                        ; CODE XREF: sub_3012F2EF+146A29j
.text:3012F300                                      ; sub_3012F2EF+146A31j ...
.text:3012F300              mov     eax, [ecx+68h]
.text:3012F303              mov     ecx, [ecx+24h]
.text:3012F306              imul    ecx, 31Ch
.text:3012F30C              mov     eax, [eax+8Ch]
.text:3012F312              mov     eax, [eax+214h]
.text:3012F318              lea     eax, [eax+ecx+0Ch]
.text:3012F31C
.text:3012F31C locret_3012F31C:                     ; CODE XREF: sub_3012F2EF+146A3Cj
.text:3012F31C              retn    4
```

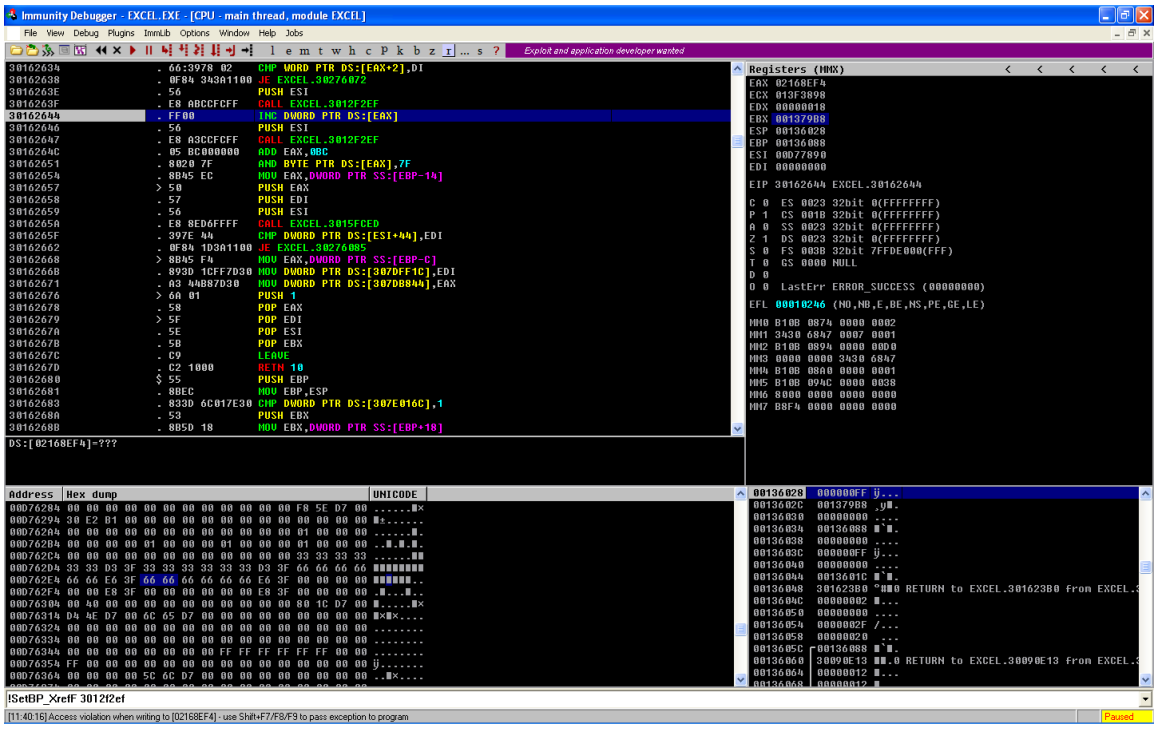
As the above code demonstrate , in case value of the 307E15A0 address equal to zero , the jump would not taken and the execution continues. At the following an address is copied to the eax register and then value this field from the iCache of SXView record is copied to the ECX register. Then the value of this field is multiplied by 796 and the result would be saved at the same ECX register. So in the following next two lines eax register contain another address and at the next line value of this address will increase with the value of eax register plus 12. (which contain multiplication of iCache field and 796)

This point can be vulnerable because of not checking the value of iCache so we can control the return value of this function that is an address.

Now we turn back to the sub_3016237B function. after that this function increment the return value of the above by one:

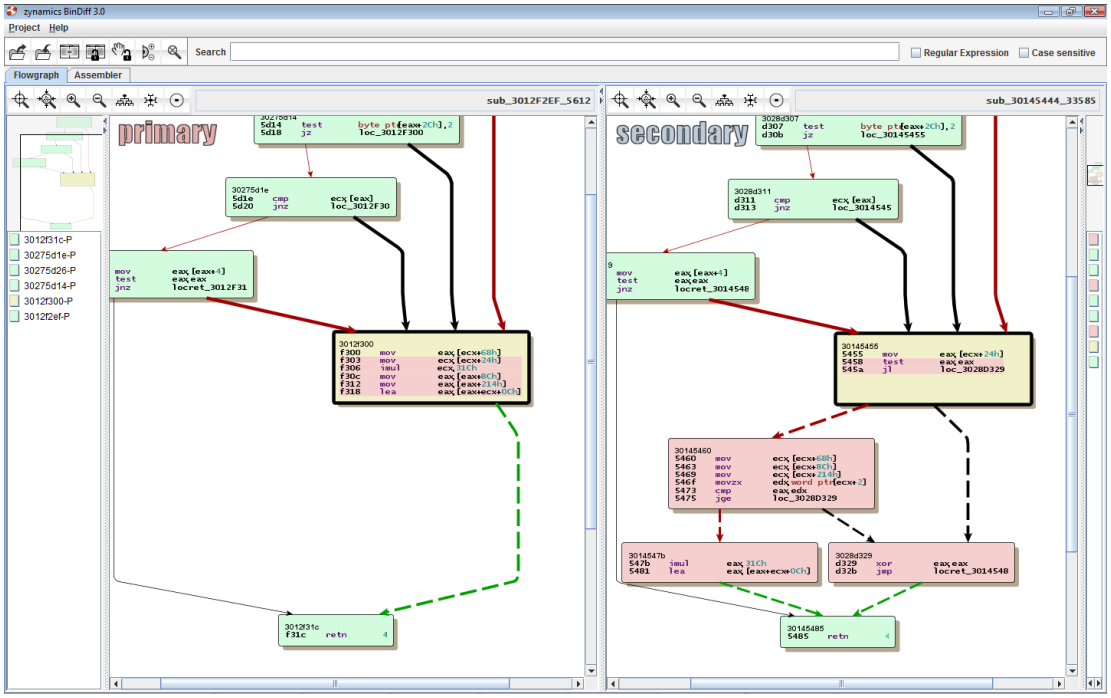
```
.text:3016263F          call    sub_3012F2EF
.text:30162644          inc     dword ptr [eax]
```

In case of invalid address our program will crash:



To crash the program you should skip 18bytes from the beginning of the record then initialize two byte to crash the program based on your value. To find the beginning of this instruction you should search ‘B0 00 3F 00’ in the hex editor. (B0 is the identity of the SXView register)

In the following graph you see a comparison between vulnerable code relating to xp sp3 and patche version. As you see some code has added to this function for checking iCache field.



Exploit

It would be possible to initialize iCache field with some value that force the next instruction rewriting an address with our arbitrary value.