Abysssec Research

1) Advisory information

Title	: Microsoft Unicode Scripts Processor Remote Code Execution (MS10-063)
Version	: usp10.dll XP, Vista
Analysis	: http://www.abysssec.com
Vendor	: http://www.microsoft.com
Impact	: Critical
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec
CVE	: CVE-2010-2738

2) Vulnerable version

Microsoft Windows XP Professional x64 Edition SP3
Microsoft Windows XP Professional x64 Edition SP2
Microsoft Windows XP Professional SP3
Microsoft Windows XP Media Center Edition SP3
Microsoft Windows XP Home SP3
Microsoft Windows Vista x64 Edition SP2
Microsoft Windows Vista x64 Edition SP1
Microsoft Windows Vista Ultimate 64-bit edition SP2
Microsoft Windows Vista Ultimate 64-bit edition SP1
Microsoft Windows Vista Home Premium 64-bit edition SP2
Microsoft Windows Vista Home Premium 64-bit edition SP1
Microsoft Windows Vista Home Basic 64-bit edition SP2
Microsoft Windows Vista Home Basic 64-bit edition SP1
Microsoft Windows Vista Enterprise 64-bit edition SP2
Microsoft Windows Vista Enterprise 64-bit edition SP1
Microsoft Windows Vista Business 64-bit edition SP2
Microsoft Windows Vista Business 64-bit edition SP1
Microsoft Windows Vista Ultimate SP2
Microsoft Windows Vista Ultimate SP1
Microsoft Windows Vista SP2
Microsoft Windows Vista SP1
Microsoft Windows Vista Home Premium SP2
Microsoft Windows Vista Home Premium SP1
Microsoft Windows Vista Home Basic SP2
Microsoft Windows Vista Home Basic SP1

Microsoft Windows Vista Enterprise SP2
Microsoft Windows Vista Enterprise SP1
Microsoft Windows Vista Business SP2
Microsoft Windows Vista Business SP1
Microsoft Windows Vista 0
Microsoft Windows Server 2008 Standard Edition SP2
Microsoft Windows Server 2008 Standard Edition 0
Microsoft Windows Server 2008 for x64-based Systems SP2
Microsoft Windows Server 2008 for x64-based Systems 0
Microsoft Windows Server 2008 for Itanium-based Systems SP2
Microsoft Windows Server 2008 for Itanium-based Systems 0
Microsoft Windows Server 2008 for 32-bit Systems SP2
Microsoft Windows Server 2008 for 32-bit Systems 0
Microsoft Windows Server 2008 Enterprise Edition SP2
Microsoft Windows Server 2008 Enterprise Edition 0
Microsoft Windows Server 2008 Datacenter Edition SP2
Microsoft Windows Server 2008 Datacenter Edition 0
Microsoft Windows Server 2003 x64 SP2
Microsoft Windows Server 2003 Web Edition SP2
Microsoft Windows Server 2003 Standard Edition SP2
Microsoft Windows Server 2003 Itanium SP2
Microsoft Windows Server 2003 Enterprise x64 Edition SP2
Microsoft Windows Server 2003 Datacenter x64 Edition SP2
Microsoft Office XP SP3
+ Microsoft Excel 2002 SP3
+ Microsoft Excel 2002 SP3
+ Microsoft FrontPage 2002 SP3
+ Microsoft FrontPage 2002 SP3
+ Microsoft Outlook 2002 SP3
+ Microsoft Outlook 2002 SP3
+ Microsoft PowerPoint 2002 SP3
+ Microsoft PowerPoint 2002 SP3
+ Microsoft Publisher 2002 SP3
+ Microsoft Publisher 2002 SP3
Microsoft Office 2007 SP2
Microsoft Office 2003 SP3
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
Avaya CallPilot Unified Messaging 0
Avaya Aura Conferencing 6.0 Standard
3DM Software Disk Management Software SP2

3) Vulnerability information

Class

1- Code execution

Impact

The Uniscribe (aka new Unicode Script Processor) implementation in USP10.DLL in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2, and Microsoft Office XP SP3, 2003 SP3, and 2007 SP2, does not properly validate tables associated with malformed OpenType fonts, which allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) Office document, aka "Uniscribe Font Parsing Engine Memory Corruption Vulnerability."

Remotely Exploitable

Yes

Locally Exploitable

Yes

4) Vulnerabilities detail

Usp10.dll module in windows and office is responsible for parsing Unicode strings. In this module there are two functions named GetCmapFontPagesPresent and LoadCmapFontGlyphs and these functions are responsible for parsing cmap table in Open Type and True Type font.

By cmap table mapping between character codes and glyph index values is established. You can get information about file formats Open Type fonts and cmap table use the following address:

http://www.microsoft.com/typography/otspec/otff.htm

http://www.microsoft.com/typography/otspec/cmap.htm

Our vulnerabilities exist in both functions and could be trigger in same way. In this analysis we will examine GetCmapFontPagesPresent function.

Cmap table for mapping operations to be able to do different characters is a different subtable. All Microsoft Unicode BMP encodings should at least have a subtable Format 4. If the font wants more support unicode characters to the Format 12 subtable also need to find. Function at the beginning GetCmapFontPagesPresent, this case is controlled by whether the desired type of subtable 12 (0xC) is or type 4 (0x4).

```
.text:74DA6C5A          mov     edi, edi
.text:74DA6C5C          push    ebp
.text:74DA6C5D          mov     ebp, esp
.text:74DA6C5F          push    ecx
.text:74DA6C60          push    ebx
.text:74DA6C61          push    esi
.text:74DA6C62          mov     esi, [ebp+arg_8]
.text:74DA6C65          mov     eax, [esi]
.text:74DA6C67          cmp     eax, 4
.text:74DA6C6A          push    edi
.text:74DA6C6B          jz      short loc_74DA6CC9
.text:74DA6C6D          cmp     eax, 0Ch
.text:74DA6C70          jnz     loc_74DA6DB1
.text:74DA6C76          xor     ebx, ebx
```

Structure Format 12 subtable (Segmented coverage) is as follows:

Type	*Name*	*Description*
USHORT	format	Subtable format; set to 12.
USHORT	reserved	Reserved; set to 0
ULONG	length	Byte length of this subtable (including the header)
ULONG	language	Please see "Note on the language field in 'cmap' subtables" in this document.
ULONG	nGroups	Number of groupings which follow

Structure of the groups is as follows:

Type	Name	Description
ULONG	startCharCode	First character code in this group
ULONG	endCharCode	Last character code in this group
ULONG	startGlyphID	Glyph index corresponding to the starting character code

More code amount is controlled field nGroups whether is greater than 0 or not.

Then the size field value nGroups, we ring the different groups to assess quality. In each group, according to the values and fields startCharCode endCharCode, another ring have done the calculation and the calculation result is stored in the buffer.

```
.text:74DA6C83              mov     edi, [ebx+eax]
.text:74DA6C86              sar     edi, 8
.text:74DA6C89              jmp     short loc_74DA6CA4
.text:74DA6C8B ; ---------------------------------------------------------------------------
.text:74DA6C8B
.text:74DA6C8B loc_74DA6C8B: : GetCmapFontPagesPresent(HDC__ *,uchar *,FONTCMAPDESC *)+53j
.text:74DA6C8B              mov     eax, edi
.text:74DA6C8D              cdq
.text:74DA6C8E              push    8
.text:74DA6C90              pop     ecx
.text:74DA6C91              idiv    ecx
.text:74DA6C93              mov     ecx, edx
.text:74DA6C95              mov     edx, [ebp+arg_4]
.text:74DA6C98              add     eax, edx
.text:74DA6C9A              mov     dl, 1
.text:74DA6C9C              shl     dl, cl
.text:74DA6C9E              or      [eax], dl
.text:74DA6CA0              mov     eax, [esi+28h]
.text:74DA6CA3              inc     edi
.text:74DA6CA4
.text:74DA6CA4 loc_74DA6CA4:                        ; CODE XREF: GetCmapFontPagesPresent(HDC__ *,uchar
*,FONTCMAPDESC *)+2Fj
.text:74DA6CA4              mov     ecx, [ebx+eax+4]
.text:74DA6CA8              sar     ecx, 8
.text:74DA6CAB              cmp     edi, ecx
.text:74DA6CAD              jle     short loc_74DA6C8B
.text:74DA6CAF              inc     [ebp+arg_8]
.text:74DA6CB2              mov     ecx, [ebp+arg_8]
.text:74DA6CB5              add     ebx, 0Ch
.text:74DA6CB8              cmp     ecx, [esi+24h]
.text:74DA6CBB              jl      short loc_74DA6C83
```

Vulnerable point of the code, lack of control levels nGroups Field Format 12 subtable and Hmchynyn startCharCode fields and values of each group is endCharCode that can be caused Array Indexing Vulnerability.

Exploit

According to the description above, if the values of fields endCharCode startCharCode and set the ring can be created with high numbers can cause stack overflow in the log.But we rewrite the return address or structure of SEH, have limitations. Because according to the loop processing operation Producer groups, values are Baznvsy amounts are limited.

We propose trigger this vulnerability through a html page. StartCharCode fields and values you need to somehow adjust endCharCode record structure of SHE, SEH Handler overwriting so that the suffering be the address from a . NET dll technology load on. then Write your shellcode within the DLL we have. Thus occur as soon as you can run an Exception to the desired location in the DLL where the shellcode is available.