Abysssec Research

1) Advisory information

Title	: Microsoft MPEG Layer-3 Audio Stack Based Overflow
Version	: l3codeca.acm (XP SP2 – XP SP3)
Analysis	: http://www.abysssec.com
Vendor	: http://www.microsoft.com
Impact	: Ciritical
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec
CVE	: CVE-2010-0480

2) Vulnerable version

Nortel Networks Symposium
Nortel Networks Contact Center NCC 0
Nortel Networks Contact Center Manager Server 0
Nortel Networks Contact Center Express
Nortel Networks Contact Center Administration 0
Nortel Networks Contact Center - TAPI Server 0
Nortel Networks CallPilot 703t
Nortel Networks CallPilot 702t
Nortel Networks CallPilot 600r
Nortel Networks CallPilot 202i
Nortel Networks CallPilot 201i
Nortel Networks CallPilot 1005r
Nortel Networks CallPilot 1002rp
Microsoft Windows XP Tablet PC Edition SP3
Microsoft Windows XP Tablet PC Edition SP2
Microsoft Windows XP Professional x64 Edition SP2
Microsoft Windows XP Professional SP3
Microsoft Windows XP Professional SP2
Microsoft Windows XP Media Center Edition SP3
Microsoft Windows XP Media Center Edition SP2
Microsoft Windows XP Home SP3
Microsoft Windows XP Home SP2
Microsoft Windows Vista Ultimate 64-bit edition SP2

Microsoft Windows Vista Ultimate 64-bit edition SP1
Microsoft Windows Vista Ultimate 64-bit edition 0
Microsoft Windows Vista Home Premium 64-bit edition SP2
Microsoft Windows Vista Home Premium 64-bit edition SP1
Microsoft Windows Vista Home Premium 64-bit edition 0
Microsoft Windows Vista Home Basic 64-bit edition SP2
Microsoft Windows Vista Home Basic 64-bit edition SP1
Microsoft Windows Vista Home Basic 64-bit edition 0
Microsoft Windows Vista Enterprise 64-bit edition SP2
Microsoft Windows Vista Enterprise 64-bit edition SP1
Microsoft Windows Vista Enterprise 64-bit edition 0
Microsoft Windows Vista Business 64-bit edition SP2
Microsoft Windows Vista Business 64-bit edition SP1
Microsoft Windows Vista Business 64-bit edition 0
Microsoft Windows Vista Ultimate SP2
Microsoft Windows Vista Ultimate 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 Server 2008 for x64-based Systems SP2
Microsoft Windows Server 2008 for x64-based Systems 0
Microsoft Windows Server 2008 for 32-bit Systems SP2
Microsoft Windows Server 2008 for 32-bit Systems 0
Microsoft Windows Server 2003 x64 SP2
Microsoft Windows 2000 Server SP4
Microsoft Windows 2000 Professional SP4
Microsoft Windows 2000 Datacenter Server SP4
Microsoft Windows 2000 Advanced Server SP4
Microsoft MPEG Layer-3 codecs 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

Successfully exploiting this issue allows remote attackers to cause denial-of-service conditions.

Remotely Exploitable

Yes

Locally Exploitable

Yes

4) Vulnerabilities detail

The flaw exists because of not properly checking a malformed AVI contains MPEG Layer-3(mp3) audio contents. In l3codecx.ax module which is a vulnerable codec there is sub_72CD1EF0 function responsible for processing data for movi section of AVI file (According to MPEGLAYER3WAVEFORMAT structure).

sub_72CD1EF0 function takes 4 arguments, first argument is address of MPEGLAYER3WAVEFORMAT structure. Second is the address of part of AVI file data which is related to mp3 file frames. Third argument is length of data. And the last argument is an address that usually equals to zero.

In part of the function value of nBlockSize field of MPEGLAYER3WAVEFORMAT structure is checked not to be 1.

```
                                                                    ...
72CD1F03        MOV AX,WORD PTR DS:[ESI+18]
72CD1F07         MOV DWORD PTR SS:[ESP+10],0
72CD1F0F        CMP AX,1
72CD1F13        JE l3codecx.72CD2079
...
```

Then third argument as length of audio data is divided by value of nBlockSize and if remainder of division equals to zero, value of fourth argument (usually zero) is substituted from length of data and compared with nBlockSize field. In case of greater than nBlockSize field the examination is continued.

```
72CD1F19        MOV ECX,DWORD PTR SS:[ESP+B4]
```

```
72CD1F20                MOV EBP,EAX
72CD1F22                AND EBP,0FFFF
72CD1F28                MOV EAX,ECX
72CD1F2A                XOR EDX,EDX
72CD1F2C                DIV EBP
72CD1F2E                TEST EDX,EDX
72CD1F30                JNZ l3codecx.72CD2080
72CD1F36                MOV EBX,DWORD PTR SS:[ESP+B8]
72CD1F3D                SUB ECX,DWORD PTR DS:[EBX]
72CD1F3F                CMP ECX,EBP
72CD1F41                JB l3codecx.72CD20AB
...
```

Then value of mp3 frame header with "41434D00" and next 4bytes after header with "63726300" is compared. If results of these comparisons are positive, we reach in to sub_72CD1DA0 function, otherwise skip it.

```
...
72CD1FA6        CMP EDX,41434D00
72CD1FAC        JNZ l3codecx.72CD2032
72CD1FB2        CMP DWORD PTR SS:[ESP+14],63726300
72CD1FBA        JNZ SHORT l3codecx.72CD2032
72CD1FBC        MOV EAX,DWORD PTR DS:[EDI+DC]
72CD1FC2        LEA ECX,DWORD PTR SS:[ESP+18]
72CD1FC6        INC EAX
72CD1FC7        MOV DWORD PTR DS:[EDI+DC],EAX
72CD1FCD        MOV EDX,DWORD PTR DS:[ESI+4]
72CD1FD0        XOR EAX,EAX
72CD1FD2        PUSH EDX
72CD1FD3        MOV AX,WORD PTR DS:[ESI+2]
72CD1FD7        PUSH EAX
72CD1FD8        PUSH ECX
72CD1FD9        MOV ECX,EDI
72CD1FDB        CALL l3codecx.72CD1DA0
...
```

In fact sub_72CD1DA0 function call, means value of nSamplePerSec field from WAWFORMATEX structure need more examination.

This function takes three arguments. First argument of that address is 144 bytes buffer. Second argument is value nChannels field form WAVEFORMATEX structure. And the third argument is value of nSamplesPerSec field. In this function known number of 144bytes buffer will be set to zero by REP STOS instruction which acts like memset function.

```
...
72CD1DA7        CMP EAX,2B11
72CD1DAC        PUSH EDI
72CD1DAD        JA SHORT l3codecx.72CD1DDB
72CD1DAF        JE SHORT l3codecx.72CD1DCD
72CD1DB1        CMP EAX,1F40
72CD1DB6        JNZ l3codecx.72CD1E88
72CD1DBC        MOV ESI,48
72CD1DC1        XOR EAX,EAX
72CD1DC3        MOV ECX,800
72CD1DC8        JMP l3codecx.72CD1E94
72CD1DCD        XOR EAX,EAX
```

```
72CD1DCF      MOV ESI,34
72CD1DD4      XOR ECX,ECX
72CD1DD6      JMP l3codecx.72CD1E94
72CD1DDB      CMP EAX,3E80
...
72CD1E88      MOV ESI,DWORD PTR SS:[ESP+1C]
72CD1E8C      MOV EAX,DWORD PTR SS:[ESP+1C]
72CD1E90      MOV ECX,DWORD PTR SS:[ESP+1C]
72CD1E94      MOV EDX,DWORD PTR SS:[ESP+18]
72CD1E98      MOV EBX,DWORD PTR SS:[ESP+14]
72CD1E9C      SUB EDX,2
72CD1E9F      MOV EDI,EBX
72CD1EA1      NEG EDX
72CD1EA3      SBB EDX,EDX
72CD1EA5      AND EDX,3
72CD1EA8      OR EDX,FFFF8840
72CD1EAE      SHL EDX,6
72CD1EB1      OR EDX,ECX
72CD1EB3      MOV ECX,ESI
72CD1EB5      MOV EBP,ECX
72CD1EB7      OR EDX,EAX
72CD1EB9      XOR EAX,EAX
72CD1EBB      SHR ECX,
72CD1EBE      REP STOS DWORD PTR ES:[EDI]
72CD1EC0      MOV ECX,EBP
72CD1EC2      AND ECX,3
72CD1EC5      REP STOS BYTE PTR ES:[EDI]
...
```

If you look at the code carefully, in the value of nSamplesPerSec field is not equal to values 2B11، EE0 ، 3E80، 5622، 5DC0، 7D00 ، AC44 and BB80, the count value indicating number of bytes that should be set to zero doesn't checked properly and will be set to value of nSamplesPerSec field. So if nSamplesPerSec is greater than 90h or 144, a stack overflow occurs.

Here is the vulnerable (secondary) and patched (primary) version of the function. As you see in the first block an instruction is added. The value of esi register at next steps would be nSamplesPerSec field. In the patched version this value first is initialized by zero so in case of inequality with those exact values, number of bytes that should be null is zero.