CVE-2004-0200: Microsoft JPEG segment length vulnerability

Kyle C. Quest
kquest@toplayer.com
Version: 1.0

This paper (which is only a small write up right now) describes some of my research findings soon after the JPEG vulnerability was disclosed. There's quite a few exploits out there right now, but no effort was made to find out more information about the actual vulnerability.

The original advisory reports that only GDIPLUS.DLL is vulnerable, which is not entirely true. I found at least two other dlls, VGX.DLL and MSO.DLL, that have a similar problem (I did it the hard way… for some reason I decided not to reverse engineer the patch). All three dlls have a similar function in them (vgx.dll and gdiplus.dll seem to have an identical function) that doesn't check the length for a copy operation.

General algorithm:

1. Dynamically allocate SegmentLength + 2 bytes from the heap (the function inserts two extra bytes in front of the data it copies from the segment to identify the segment type).
2. Copy the segment type into the first 2 bytes.
3. Copy the segment length field (another 2 bytes).
4. Calculate the length of the segment data to copy: SegmentLength – 2.
5. Copy segment data.

Step 4 is where the vulnerability is located as we all know.

```
lea     eax, [esi+2]
push    eax
call    sub_588518
test    eax, eax
mov     [ebp+lpMem], eax
jz      loc_5CC58A
mov     cx, word ptr [ebp+arg_4]
mov     [eax], cx
mov     cx, word ptr [ebp+arg_0]
lea     edx, [esi-2] ; Len-2 bug!
. . .
mov     ecx, edx
mov     eax, ecx
shr     ecx, 2
rep movsd
```

The original advisory also didn't mention that the bug can be triggered not only with segments identified by "0xff 0xfe", but also *0xff 0xed*, *0xff 0xe1*, and *0xff 0xe2*. (I think this is already known though).

The fact that the vulnerability is present not only in GDIPLUS.DLL, but also VGX.DLL (IE) and MSO.DLL (MS Office), means that there are additional attack vectors that make it possible to easily attack not only Windows XP users, but also Windows 2000 users. In one such case, an attacker can setup a webpage that uses VGX.DLL (which I have done in my private tests) infecting everybody who visits it (WinXP/Win2K with the correct version of IE installed).

I will add more information about the vulnerable functions and the heap memory management functions to better explain what is going on and what the data flow is like in the later edition of this paper (once I have free time to write it all down). Meanwhile, if you want to disassemble the vulnerable functions yourself here's some info that will be useful when you are looking for them:

GDIPLUS.DLL (5.1.3097.0) RVA:
0x7A1A9921

MSO.DLL (10.0.3501) RVA:
0x30D4088D

VGX.DLL (6.00.2800.1106) RVA:
0x5CC46A

NOTE: The current version of the document can be found at: www.unital.com/research/ms_jpeg.pdf