Module 1.2

More Control Hijacking Attacks: Integer Overflow

Control Hijacking

Integer Overflow

More Hijacking Opportunities

- **Integer overflows**: (e.g. MS DirectX MIDI Lib)
- **Double free**: double free space on heap
  - Can cause memory mgr to write data to specific location
  - Examples: CVS server
- **Use after free:** using memory after it is freed
- **Format string vulnerabilities**

Integer Overflows (see Phrack 60)

Problem: what happens when int exceeds max value?

int m; (32 bits) short s; (16 bits) char c; (8 bits)

c = 0x80 + 0x80 = 128 + 128 ⇒ c = 0

s = 0xff80 + 0x80 ⇒ s = 0

m = 0xffffff80 + 0x80 ⇒ m = 0

Can this be exploited?

An example

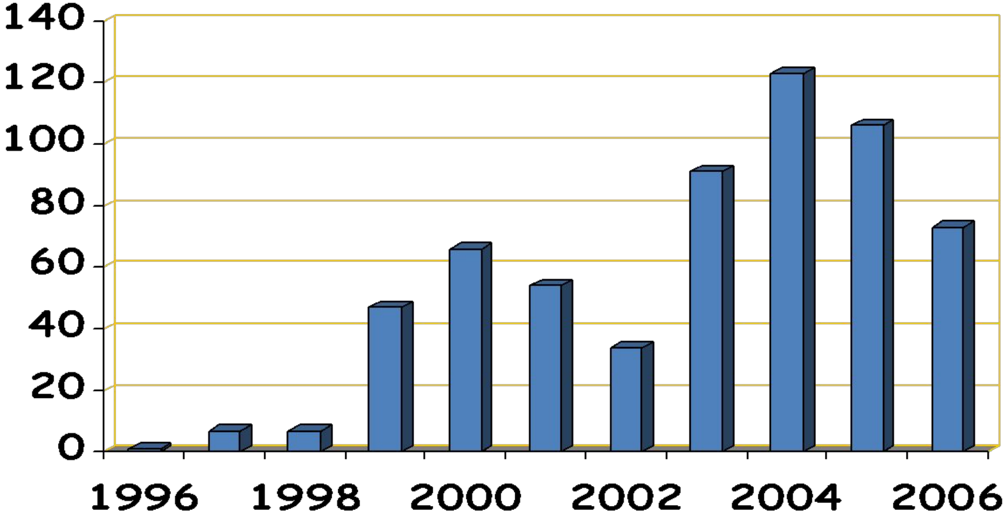
```
void  func( char *buf1, *buf2,    unsigned int len1, len2) {
        char temp[256];
        if  (len1 + len2 > 256)  {return -1}       // length check
        memcpy(temp, buf1, len1);   // cat buffers
        memcpy(temp+len1, buf2, len2);
        do-something(temp);       // do stuff
}
```

What if **len1 = 0x80,** **len2 = 0xffffff80** ?

⇒ len1+len2 = 0

Second memcpy() will overflow heap !!

Integer overflow exploit stats



Source: NVD/CVE