Subject: Re: Server crash dump
Posted by iRANian on Thu, 06 Jun 2013 18:03:52 GMT
View Forum Message <> Reply to Message

Crashed in MDB_SSGM_KeyHook_Clone::Destroyed(GameObject *obj) while Calling ::RemoveHook, which I added to the plugin by copying it from the SSGM 2.0.2 source:

```
void MDB_SSGM_KeyHook_Clone::Destroyed(GameObject *obj) {
 if (is_keyhook_set == 1337) {
  RemoveHook();
 }
}

void MDB_SSGM_KeyHook_Clone::RemoveHook() {
 if (hookid != 0 && RemoveKeyHook != 0) {
  RemoveKeyHook(hookid);
  hookid = 0;
  if (k != 0) {
   delete[] k->key;
   delete k;
   k = 0;
  }
 }
}
```

```
    70: void MDB_SSGM_KeyHook_Clone::Destroyed(GameObject *obj) {
730F12A0 56                   push        esi
730F12A1 8B F1                mov         esi,ecx
    71:  if (is_keyhook_set == 1337) {
730F12A3 81 7E 24 39 05 00 00 cmp         dword ptr [esi+24h],539h
730F12AA 75 45                jne         MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)
    72:   RemoveHook();
730F12AC 8B 46 20             mov         eax,dword ptr [esi+20h]
730F12AF 85 C0                test        eax,eax
730F12B1 74 3E                je          MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)
730F12B3 8B 0D F0 20 0F 73    mov         ecx,dword ptr [__imp_RemoveKeyHook (730F20F0h)]
730F12B9 8B 09                mov         ecx,dword ptr [ecx]
730F12BB 85 C9                test        ecx,ecx
730F12BD 74 32                je          MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)
730F12BF 50                   push        eax
730F12C0 FF D1                call        ecx
730F12C2 8B 46 1C             mov         eax,dword ptr [esi+1Ch]
730F12C5 83 C4 04             add         esp,4
730F12C8 C7 46 20 00 00 00 00 mov         dword ptr [esi+20h],0
730F12CF 85 C0                test        eax,eax
730F12D1 74 1E                je          MDB_SSGM_KeyHook_Clone::Detach+51h (730F12F1h)
730F12D3 8B 50 04             mov         edx,dword ptr [eax+4]  // CRASHES HERE
730F12D6 52                   push        edx
730F12D7 FF 15 80 20 0F 73    call        dword ptr [__imp_operator delete[] (730F2080h)]
730F12DD 8B 46 1C             mov         eax,dword ptr [esi+1Ch]
730F12E0 50                   push        eax
730F12E1 FF 15 88 20 0F 73    call        dword ptr [__imp_operator delete (730F2088h)]
730F12E7 83 C4 08             add         esp,8
730F12EA C7 46 1C 00 00 00 00 mov         dword ptr [esi+1Ch],0
730F12F1 5E                   pop         esi
    73:  }
    74: }
```

Registers:

```
  EDX 730F22F0
  EAX 0000001F
  EBP 0018FAF0
  AL 1F
```

The value of the 'k' pointer variable (which is of type KeyHookStruct)somehow was set to 0x1F instead of a valid pointer address, then the code tries to access memory address variable 'k' + 4 (0x1f + 4) which is invalid and the server crashed.