
Subject: Re: [Plug-in] SSGM2.02 Ping Plugin
Posted by [jnz](#) on Tue, 16 Nov 2010 12:30:30 GMT
[View Forum Message](#) <> [Reply to Message](#)

That Get_Part_Names function can be exploited, if a player's name has a substring of another player's name then Get_Part_Name will always fail for the substring. IE:

```
jnz joins the game
jnzkiller joins the game
```

```
Get_Part_Names("jnz"); //returns 0
```

Also note that it would be worth changing stricmp and strstr to strcmp and strstr, I am not sure but I think 2 players can join with the same name but in different case. ("jnz", "JNZ"). If this is not the case then just ignore me.

A fix would be:

```
GameObject *Get_Part_Name(const char *name1)
{
    GenericSLNode *x = BaseGameObjList->HeadNode;
    int count = 0;
    GameObject *current = 0;
    while (x)
    {
        GameObject *o = As_ScriptableGameObj((GameObject *)x->NodeData);
        if (o && Commands->Is_A_Star(o) && As_SoldierGameObj(o)){
            const char *name = Get_Player_Name(o);
            if(stricmp(name, name1) != 0)
            {
                delete []name;
                return o;
            }
            if (strstr(name,name1))
            {
                current = o;
                count++;
            }
            delete[] name;
        }
        x = x->NodeNext;
    }
    if ((count == 1) && (current) && (Commands->Get_ID(current)))
    {
        return current;
    }
    else
```

```
{  
  return 0;  
}  
}
```
