Remote Mouse 3.008 Arbitrary Remote Command Execution Exploit

Date: 03/08/2024
Prepared by: Miftahul Huq

Overview:

This document details the exploitation of an arbitrary remote command execution vulnerability in Remote Mouse version 3.008 (EDB-ID 46697). Due to insufficient authentication mechanisms, an attacker can execute unauthorized commands on a Windows system. We provide a controlled demonstration of this exploit by remotely launching the calculator application on the affected machine, illustrating the severity of the vulnerability.

Target Software:

- Name: Remote Mouse
- Version: 3.008
- Platform: Windows
- Exploit Database Link: EDB-ID 46697
- Vulnerability: Arbitrary Remote Command Execution

Requirements:

- A Windows host with Remote Mouse version 3.008 installed and running
- A separate host with Python 2.7 (Kali Linux is used in this scenario)
- Network access from the Python host to the Windows host

Installation & Configuration:

1. Ensure that Remote Mouse version 3.008 is installed and running on the target Windows machine. You can download the .exe file by going to the exploit database link above and then clicking the down arrow button next **“Vulnerable App.”** Run the .exe file, keep all the default options, and follow the normal installation process. It’s pretty straight forward.
2. Note down the IP address of the Windows machine running Remote Mouse.
3. On the Kali Linux machine, save the provided Python script and bash scripts, *exploit.py and run_exploit.sh*.

4. Make sure Python 2.7 is installed on the Kali Linux machine. You can verify this by running python2 --version.

Exploit Usage:

1. On the Kali Linux machine, navigate to the directory containing the scripts.
2. Run the *run_exploit.sh* script with the target IP address as the argument. Make sure that both exploit.py and run_exploit.sh files are in the same directory.
3. The script will attempt to connect to the Remote Mouse service and execute the calculator application (calc.exe) on the Windows machine as a proof of concept.

Script Breakdown of exploit.py (A modification has be been to the script to just run the PopCalc() function):

- The script performs the following actions:
- Ping Function: Checks if the Remote Mouse service is running on the target machine.
- MoveMouse Function: Moves the mouse cursor on the target machine.
- MousePress Function: Simulates a mouse press on the target machine.
- SendString Function: Sends a string of characters as keystrokes to the target machine.
- PopCalc Function: A wrapper that calls the necessary functions to open the calculator app.

Notes:

- The exploitation script is a proof of concept.
- The actual mouse movement and keystrokes may vary depending on the screen resolution and layout of the target machine.
- The delay between commands in the script may need to be adjusted based on network latency and the responsiveness of the target machine.

Video Demonstration:

The following link is a video recording that demonstrates the successful execution of the exploit on the target system.

VIdeo Link:
https://rit.zoom.us/rec/share/eM99OAfpFDdibnFndI9Txal06aeX68fwlY45X0JmjHtdFisD6XuwlEwXHhliKoga.nB27-s6mp0qhL2BX