CVE-2024-6387 OpenSSH 重大

OpenSSH含有可遠端攻陷伺服器的回歸漏洞

> OpenSSH團隊於7月1日發布的OpenSSH 9.8/9.8p1版本，修補編號CVE-2024-6387的高風險漏洞，允許駭客在不需要身分驗證的情況下，自遠端

資料來源：

https://www.ithome.com.tw/news/163737

https://www.qualys.com/regresshion-cve-2024-6387/

受影響 OpenSSH 版本

> 除 **4.4p1 ~ 8.5p1**、**9.8p1** 不受影響，其餘版本皆具此漏洞

緊急應對措施

⚠ 檢查**Firewall Policy**，禁止主機**SSH**對外開放 ⚠

⚠ 檢查**Firewall Policy**，禁止主機**SSH**對外開放 ⚠

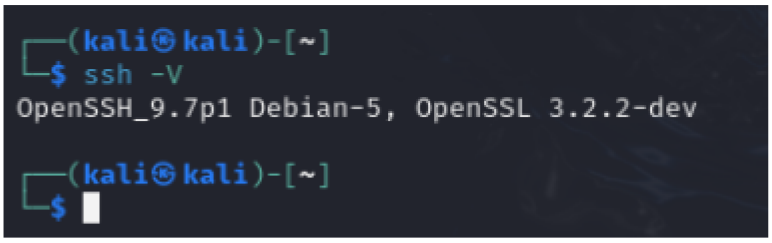
⚠ 檢查**Firewall Policy**，禁止主機**SSH**對外開放 ⚠

(很重要說三遍)

檢查SSH版本

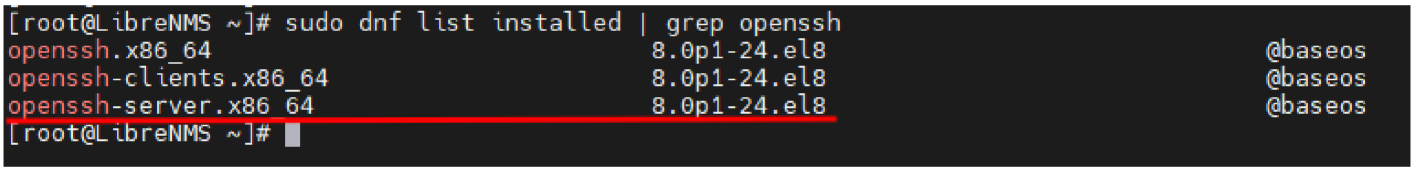
一、透過 ssh -V 檢查 (需登入、一次一台)

```
ssh -V
```



二、透過 dnf / apt 檢查 (需登入、一次一台)

```
<< Redhat / CentOS / Rocky / Oracle >>
sudo dnf list installed | grep openssh

<< Debian / Ubuntu >>
sudo apt list --installed | grep openssh
```



三、透過NMap檢查 (不需登入、可多台)

```
sudo nmap -A -sT -T4 -p 22 192.168.xx.xx/24
```

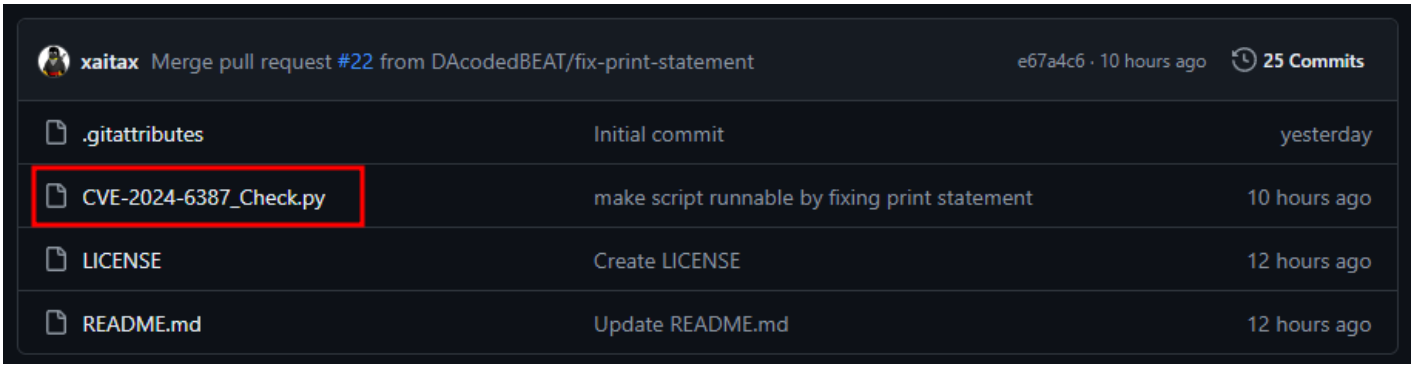
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nmap -A -sT -T4 -p 22 192.168.123.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 23:17 CST
Nmap scan report for 192.168.123.104
Host is up (0.00075s latency).

PORT   STATE  SERVICE VERSION
22/tcp closed ssh
MAC Address: [redacted] (Universal Global Scientific Industrial)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.75 ms 192.168.123.104

Nmap scan report for 192.168.123.240
Host is up (0.00036s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|  [redacted]
|_
MAC Address: [redacted] (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 - 3.10 (96%), Linux 3.10 (95%), Linux 3.12 - 4.10 (95%), Linux 3.1 (95%), L
inux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 2.6.18 (94%), Geovision EBD4700 CCT
V camera (Linux 3.4) (93%), Western Digital My Cloud DL4100 NAS (Linux 3.10) (93%), ASUS RT-N56U WAP (Linux 3.4
) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.36 ms 192.168.123.240

Nmap scan report for 192.168.123.241
Host is up (0.00068s latency).

PORT   STATE SERVICE VERSION
```

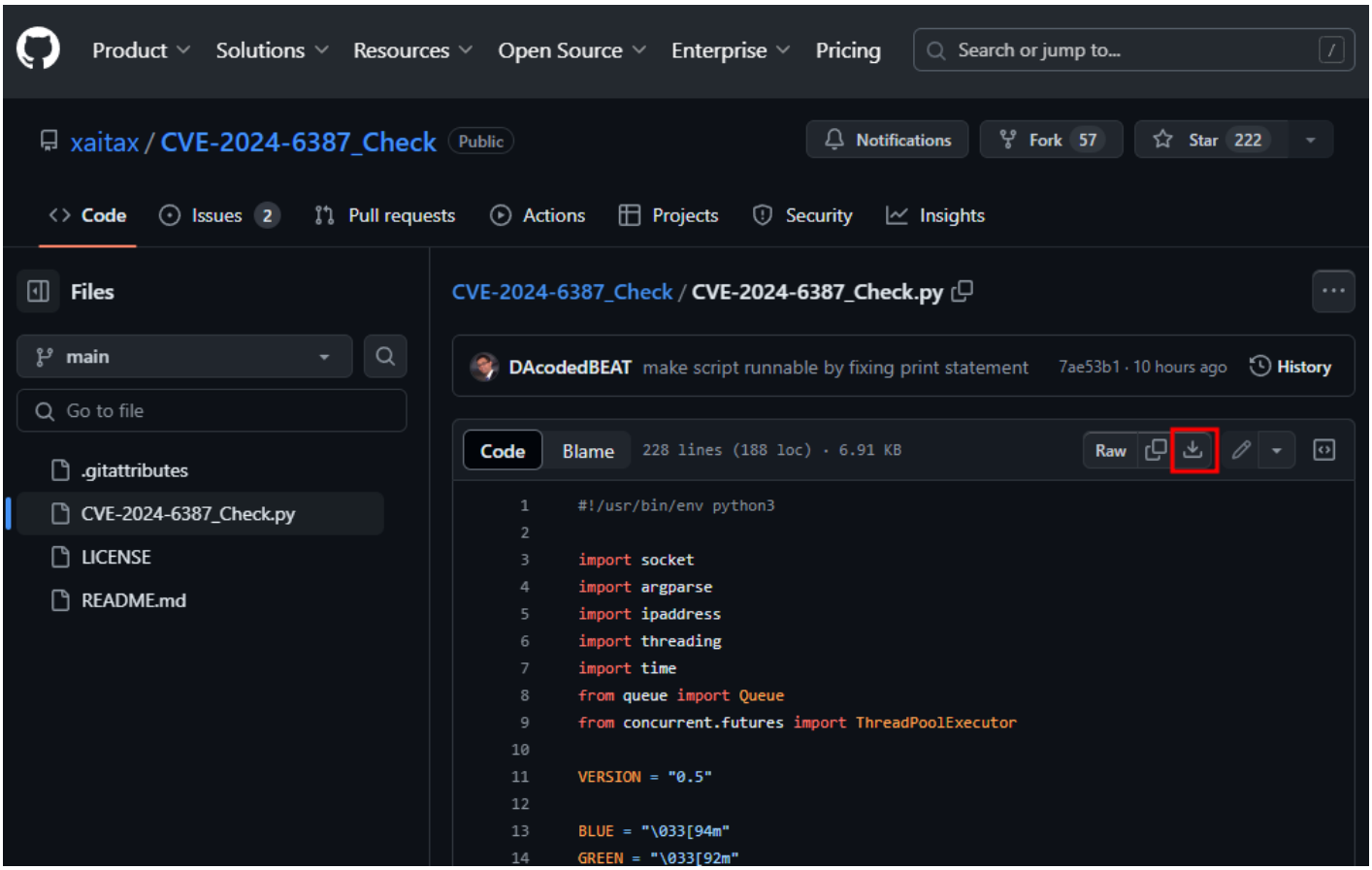
□□Github Open Source Tool (□□□□□□□□)

□□□**CVE-2024-6387_Check**

https://github.com/xaitax/CVE-2024-6387_Check

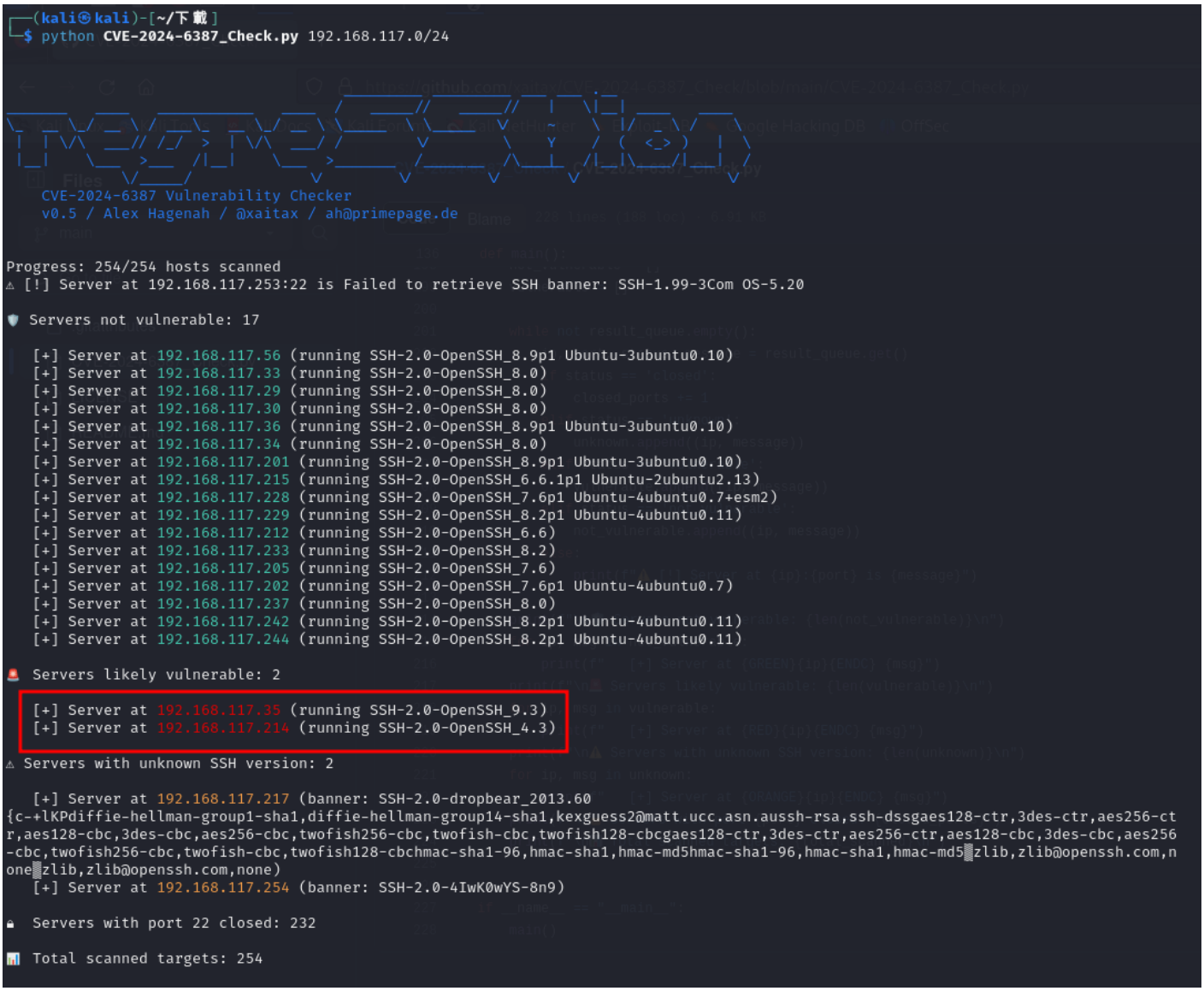
□□□□□□□





□□□□□□□□□

```
python CVE-2024-6387_Check.py 192.168.xx.xx/24
```



"□□"□□□□□□□□

□□□

⚠ □□□OpenSSH□9.8p1□□ ⚠

⚠ □□□OpenSSH□9.8p1□□ ⚠

⚠ □□□OpenSSH□9.8p1□□ ⚠

(□□□□□□)

Revision #7
Created 2 July 2024 15:27:14 by □□□
Updated 3 July 2024 08:19:36 by □□□