

# CVE-2024-6387 OpenSSH

## OpenSSH

“ OpenSSH  7  1  OpenSSH 9.8/9.8p1  CVE-2024-6387 

 :

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

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

## OpenSSH

 4.4p1 ~ 8.5p1  9.8p1 



  Firewall Policy  SSH  

  Firewall Policy  SSH  

  Firewall Policy  SSH  

()

## SSH

## ssh -V ( )

```
ssh -V
```

```
(kali@kali)-[~]
└─$ ssh -V
OpenSSH_9.7p1 Debian-5, OpenSSL 3.2.2-dev

(kali@kali)-[~]
└─$
```

## dnf / apt ( )

<< Redhat / CentOS / Rocky / Oracle >>

```
sudo dnf list installed | grep openssh
```

<< Debian / Ubuntu >>

```
sudo apt list --installed | grep openssh
```

```
[root@LibreNMS ~]# sudo dnf list installed | grep openssh
openssh.x86_64                               8.0p1-24.el8 @baseos
openssh-clients.x86_64                     8.0p1-24.el8 @baseos
openssh-server.x86_64                      8.0p1-24.el8 @baseos
[root@LibreNMS ~]#
```

```
(kali@kali)-[~/Downloads]
└─$ sudo apt list --installed | grep openssh
[sudo] password for kali:

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

openssh-client/kali-rolling,now 1:9.7p1-5 amd64 [installed]
openssh-server/kali-rolling,now 1:9.7p1-5 amd64 [installed,automatic]
openssh-sftp-server/kali-rolling,now 1:9.7p1-5 amd64 [installed,automatic]

(kali@kali)-[~/Downloads]
└─$
```

## NMap ( )

```
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%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 2.6.18 (94%), Geovision EBD4700 CCTV 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](https://github.com/xaitax/CVE-2024-6387_Check)

📄📄📄📄

xaitax Merge pull request #22 from DAcodedBEAT/fix-print-statement		e67a4c6 · 10 hours ago	🕒 25 Commits
📄 .gitattributes	Initial commit		yesterday
📄 CVE-2024-6387_Check.py	make script runnable by fixing print statement		10 hours ago
📄 LICENSE	Create LICENSE		12 hours ago
📄 README.md	Update README.md		12 hours ago

Product Solutions Resources Open Source Enterprise Pricing Search or jump to...

xaitax / CVE-2024-6387\_Check Public Notifications Fork 57 Star 222

Code Issues 2 Pull requests Actions Projects Security Insights

Files main Go to file

- .gitattributes
- CVE-2024-6387\_Check.py
- LICENSE
- README.md

CVE-2024-6387\_Check / CVE-2024-6387\_Check.py

DAcodedBEAT make script runnable by fixing print statement 7ae53b1 · 10 hours ago History

Code Blame 228 lines (188 loc) · 6.91 KB Raw Copy Download Edit

```
1 #!/usr/bin/env python3
2
3 import socket
4 import argparse
5 import ipaddress
6 import threading
7 import time
8 from queue import Queue
9 from concurrent.futures import ThreadPoolExecutor
10
11 VERSION = "0.5"
12
13 BLUE = "\033[94m"
14 GREEN = "\033[92m"
```



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

